Available online at www.ijournalse.org

Emerging Science Journal

(ISSN: 2610-9182)

Vol. 9, No. 5, October, 2025

Integrated AI, IoT, and Blockchain for Enhancing Security and Traceability in Perishable Logistics

William Villegas-Ch [1*], Rommel Gutierrez [1], Jaime Govea [1], Joselin García-Ortiz [1]

[1] *Escuela de Ingeniería en Ciberseguridad, FICA, Universidad de Las Américas, Quito 170125, Ecuador.*

Abstract

The perishability of food products in the supply chain poses a significant challenge in ensuring quality and safety. Inefficient monitoring of temperature, humidity, and storage time results in substantial economic losses and increased health risks. Traditional traceability systems rely on manual audits or essential IoT platforms that lack predictive capabilities, leading to delayed anomaly detection and inefficient intervention. Blockchain-based solutions improve transparency but primarily focus on record verification rather than active anomaly detection and automated decision-making. This study proposes an integrated system combining Artificial Intelligence (AI), the Internet of Things (IoT), and blockchain to optimize food traceability through real-time monitoring, predictive analytics, and secure decentralized record management. The system deploys smart sensors across storage and transportation units to continuously collect environmental data, which is processed by a deep learning model trained to detect deviations with 92.4 % accuracy. Detected anomalies trigger automated responses via smart contracts in a blockchain network, ensuring immediate corrective actions while maintaining immutable audit records. Results demonstrate a 64.3 % reduction in response time, improving reaction efficiency to critical storage failures. Additionally, false positive alerts decreased by 73.1 %, optimizing operational efficiency and minimizing unnecessary interventions. The blockchain implementation reduced storage overhead by 76.9%, ensuring scalability and long-term feasibility. This research establishes a foundation for intelligent, automated food supply chain management, demonstrating that integrating AI, IoT, and blockchain enhances safety, reduces waste, and optimizes logistics. Future work will focus on improvements in large-scale deployment and computational efficiency to refine this innovative approach.

Keywords:

Intelligent Food Traceability;
AI-Driven Anomaly Detection;
Blockchain for Supply Chain;
IoT-Based Cold Chain Monitoring.

Article History:

Received:	20	March	2025
Revised:	22	July	2025
Accepted:	04	August	2025
Published:	01	October	2025

1- Introduction

Monitoring and traceability in the supply chain of perishable products continue to represent a significant challenge in the food industry, where ensuring product quality and safety depends on the ability to identify and respond in real-time to changes in environmental conditions [1]. Factors such as temperature, humidity, and inadequate storage times can compromise product integrity, generating significant economic losses and risks to public health [2]. Although traditional systems have relied on manual records or basic Internet of Things (IoT) platforms, their lack of predictive capabilities limits early anomaly detection and effective response strategies.

This study proposes a hybrid system that integrates Artificial Intelligence (AI), IoT, and blockchain technologies to address these shortcomings by combining real-time monitoring, advanced predictive analytics, and immutable data records within a decentralized infrastructure [3]. Unlike conventional approaches, this solution incorporates optimized IoT sensors with efficient communication protocols such as Wi-Fi, LoRaWAN, and 5G, deep learning models trained

* **CONTACT**: william.villegas@udla.edu.ec

DOI: http://dx.doi.org/10.28991/ESJ-2025-09-05-011

to detect anomalous storage and transport conditions, and a blockchain network to automatically register critical events, ensuring both immutability and verifiability of the information [4, 5].

The scientific literature has documented the need to improve traceability in the food industry [6]. Previous studies have explored the application of blockchain to ensure transparency in the supply chain. Still, most approaches are limited to passive record verification, lacking active detection and autonomous decision-making capabilities supported by AI [7]. Similarly, existing IoT-based systems provide real-time data collection but do not include robust analytical frameworks to anticipate failures in preservation. The integration of these three technological pillars addresses these limitations. It represents a significant step forward, enabling the secure acquisition and storage of data and the automation of responses to critical scenarios [8].

The proposed model has been validated through controlled experiments in an environment that simulates the operating conditions of a food supply chain. IoT sensors have been implemented at different points in the logistics network, including refrigeration chambers, transport units, and distribution warehouses, collecting real-time data on temperature, humidity, and storage cycles. This data has been analyzed using a deep learning model designed to detect anomalies with an accuracy of 92.4%, representing a substantial improvement over conventional systems based on predefined thresholds.

One of this study's most relevant findings is improving system latency. While in traditional systems, the average response time to an anomalous event is 8.7 seconds, the proposed model reduces this time to 3.1 seconds, equivalent to a 64.3 % improvement in reaction capacity. In addition, optimizing blockchain records has reduced the data storage size by 76.9 %, which favors the system's scalability without compromising the security or integrity of the records.

Another key aspect of the research is the system's ability to reduce false positives in anomaly detection by 73.1 %, which minimizes unnecessary interventions and improves operational efficiency. This reduction results from training the AI model with data from multiple test environments, allowing it to distinguish between normal variations and events that compromise product quality. Regarding infrastructure, the system has been designed to ensure interoperability with different logistics platforms. Implementing smart contracts on the blockchain allows the automated execution of processes without human intervention, ensuring critical decisions, such as activating backup refrigeration systems or generating alerts for logistics operators, are carried out efficiently and verifiably [9].

This study significantly contributes to the scientific community and the food industry. Combining emerging technologies in a comprehensive solution demonstrates that it is possible to improve food traceability and safety in an automated and highly efficient manner. Furthermore, the system is scalable and adaptable to other sectors, such as the pharmaceutical industry, where traceability and environmental condition control are equally critical to ensure product quality and safety.

This work is structured as follows: the materials and methods section describes the system architecture, the data acquisition and processing methodology, the AI models used, and the blockchain implementation for secure record management. The results section presents key findings from the system evaluation, including accuracy metrics, data transmission efficiency, and operational cost reduction. The discussion section contextualizes these findings about previous studies, highlighting the improvements obtained and analyzing the system's limitations. Finally, the conclusions section summarizes the research contributions and raises possible directions for future improvements and applications of the model.

2- Literature Review

Integrating advanced technologies such as AI, IoT, and blockchain has revolutionized traceability and security in the perishable product supply chain. According to a study by Liu et al., blockchain technology has emerged as a key tool to ensure transparency and security in the food supply chain. Liu et al. [10] proposes a blockchain-based architecture to improve the traceability of agricultural products. The authors developed a system that records each stage of the production and distribution process on a blockchain, ensuring the immutability and verifiability of the data. The results demonstrated a significant reduction in product tracking time, improving efficiency and trust in the supply chain.

On the other hand, Tang et al. [11] investigated the integration of blockchain with smart contracts to automate processes in the perishable product supply chain. Their approach allowed the automatic execution of predefined actions under specific conditions, such as detecting out-of-range temperatures during transportation. This automation improved the response to critical events and reduced human intervention, minimizing errors and operational costs. IoT has facilitated continuous monitoring of environmental conditions in the supply chain. Sarkar et al. [12] developed an IoT sensor network to monitor temperature and humidity while transporting perishable foods. The collected data was transmitted in real-time to a centralized platform, allowing immediate detection of deviations and implementation of corrective measures. This approach resulted in a 15 % decrease in product losses due to inadequate storage and transportation conditions. Furthermore, Javadi et al. [13] explored combining IoT with 5G technology to improve the

speed and reliability of data transmission in the food supply chain. Implementing this infrastructure enabled faster and more stable communication between devices, optimized data synchronization, and improved real-time responsiveness to detectable anomalies.

AI has been instrumental in analyzing large volumes of data generated by IoT devices. Fiore & Mongiello [14] presented a deep learning model to identify anomalous supply chain sensor data patterns. Their system achieved 94 % accuracy in detecting conditions that could compromise product quality, enabling proactive interventions and significantly reducing losses. In a related study by Ramkumar et al. [15] implemented machine learning algorithms to predict failures in refrigeration equipment used to store perishable products. By anticipating potential breakdowns, companies could perform preventive maintenance, avoiding interruptions in the cold chain and ensuring the freshness of food until its destination.

Despite the advances above, integrating these technologies faces challenges. Interoperability between different systems and standards, scalability of blockchain solutions, and efficient management of data generated by IoT devices require continued attention. Future research could focus on developing universal communication protocols, optimizing blockchain consensus algorithms to handle higher transaction volumes, and improving big data analytics techniques to extract actionable insights in real-time.

The proposed system is theoretically grounded in cyber-physical systems (CPS) principles and distributed intelligent architectures. At its core, the model is structured in three integrated layers: perception, processing, and verification. The perception layer, composed of IoT sensors, continuously captures environmental variables critical to perishable logistics, such as temperature and humidity. This aligns with the CPS paradigm, where embedded systems interact in real time with the physical world to provide actionable data [16]. The processing layer, driven by AI, introduces learning capabilities through deep neural networks that enable contextualized anomaly detection and adaptive decision-making. This learning process improves system responsiveness and reliability, allowing for identifying abnormal patterns beyond predefined thresholds [17].

Blockchain technology ensures data immutability, transparency, and decentralized auditing at the verification layer. Integrating smart contracts adds a layer of algorithmic governance that supports autonomous event response and secure execution of business rules without human intervention [7]. By combining these layers, the system establishes a closed-loop framework in which perception feeds intelligent analysis and verified decisions trigger secure and traceable actions across the network. This architecture contrasts with conventional traceability systems by embedding intelligence into the data flow and audit process [10]. Moreover, using optimized data structures such as Merkle trees within the blockchain layer enhances the system's scalability and auditability, making it viable for deployment in dynamic and resource-constrained environments [18]. This foundation supports shifting from passive traceability toward intelligent, proactive, and verifiable supply chain management.

3- Material and Methods

3-1- Description of the Study Environment

The food industry faces significant challenges in the traceability and quality control of perishable products, especially in monitoring their storage and transport conditions. Food stability depends on physical and environmental parameters that must be maintained within specific ranges to avoid premature degradation, microbial proliferation, and loss of organoleptic properties [19]. Inefficient monitoring of these parameters compromises consumer safety, increases the risk of contamination, and generates considerable economic losses. A real-time traceability system makes detecting deviations in optimal conservation conditions possible, ensuring efficient management throughout the supply chain [20].

The developed system focuses on the traceability of fruits, vegetables, and meat products, selected for their high sensitivity to temperature, humidity, and storage time variations. In the case of fruits and vegetables, product stability depends on temperature regulation of 1 to 10 °C, depending on the crop type and its post-harvest respiration rate. Relative humidity must be maintained between 85 % and 95 % to prevent weight loss and dehydration of cellular tissue. During storage and transport, fruits and vegetables may be exposed to temperature variations of ±3 °C, accelerating ethylene production and premature ripening.

Meat products have more stringent storage requirements [21]. The storage temperature of fresh meat must be maintained between -1 °C and 4 °C, while for frozen beef, temperatures below -18 °C are required to prevent bacterial growth and protein degradation. Relative humidity in cold storage chambers ranges between 75 % and 85 %, depending on the type of meat and the permitted storage time. Any variation greater than ±1 °C in these products increases the risk of proliferation of microorganisms such as Salmonella, Listeria monocytogenes, and Escherichia coli, compromising the final product's safety [22].

The transportation of these foods constitutes a critical phase within the supply chain since thermal fluctuations and failures in refrigeration systems can occur during this process. The transportation time varies according to the distance between the point of production and the destination, ranging from 4 to 48 hours for local distribution and between 48 and 120 hours for exports. During this period, the internal temperature of the refrigerated container must be kept stable

with a maximum tolerance of ±0.5 °C for meat and ±2 °C for fruits and vegetables. Thresholds temperature exceeds these thresholds; biochemical alterations are generated in the product, which reduces its shelf life and affects its commercial quality.

The proposed system implements a network of IoT sensors at strategic points along the supply chain, including storage areas and transport units, to capture real-time data on temperature, humidity, and storage time [16]. These data are processed by artificial intelligence algorithms that identify patterns of deviation in storage conditions and predict possible failures in the cold chain. Each traceability record is stored in a blockchain network, guaranteeing the immutability of the information and allowing automated audits through smart contracts. This technological integration ensures that each food product batch maintains the appropriate conditions from its origin to the final consumer, minimizing losses and optimizing quality at each process stage.

3-2- Architecture of the Proposed System

The integration of IoT, AI, and Blockchain in the traceability of perishable products allows the development of a robust monitoring system capable of recording and analyzing in real-time the environmental conditions that affect the quality and safety of food. The developed architecture covers data capture at strategic points in the supply chain, the application of artificial intelligence models for detecting deviations, and the use of blockchain to guarantee the immutability and traceability of records. Figure 1 presents the system's architecture, which illustrates the flow of data from acquisition to the display of information on the user interface.

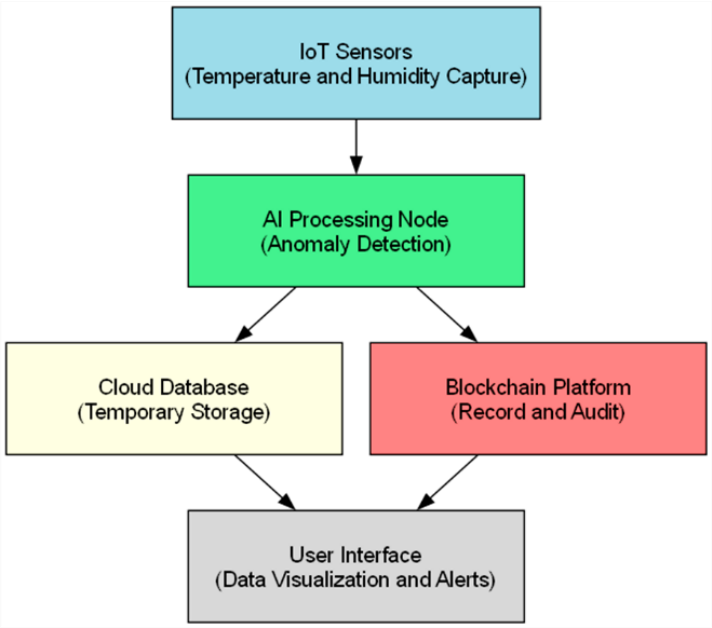


Figure 1. Architecture of the Traceability System Based on IoT, AI, and Blockchain

The system comprises five main modules: the data acquisition layer, the artificial intelligence processing node, the cloud database, the blockchain platform, and the user interface. Each module plays a specific role in the traceability chain and is interconnected by a communication infrastructure designed to minimize data transmission latency and ensure system reliability.

The IoT sensors used in the data acquisition layer are designed for real-time capture of temperature and humidity using communication technologies such as LoRaWAN, Zigbee, or LTE-M, depending on the operating conditions of the environment [23]. These sensors are in storage and transport areas, ensuring complete coverage of the conditions to which perishable products are exposed. The measurements have an adaptable sampling frequency, with intervals between 30 seconds and 5 minutes, depending on the environment's thermal stability and the product's sensitivity to environmental variations. The data is transmitted to an intermediate processing node, where an initial verification is carried out to filter out erroneous readings or inconsistencies before being processed by the AI models.

The AI processing node runs advanced anomaly detection models based on supervised and unsupervised machine learning algorithms optimized for time series analysis. Recurrent Neural Networks (RNN) and AutoRegressive Integrated Moving Average (ARIMA) models predict deviations in temperature and humidity, allowing the identification of patterns that suggest failures in refrigeration systems or exposure to inadequate conditions [24]. The model architecture is based on an early detection scheme, where dynamic thresholds are established based on product characteristics and previous environmental conditions.

The processed and validated data are stored in a cloud database, which operates under a distributed storage scheme to ensure availability and scalability. A hybrid storage model is implemented, where frequently queried data remains on fast-access servers while historical records are stored on long-term storage systems optimized for massive queries. The cloud infrastructure acts as an intermediary between the AI node and the blockchain platform, facilitating data aggregation and reducing the volume of information recorded on the blockchain [25].

The blockchain platform constitutes the core of the traceability system, guaranteeing records' immutability and the information's decentralization. An architecture based on Hyperledger Fabric is used due to its ability to operate with defined permissions and its optimization for fast transactions in industrial environments. Each batch of perishable products receives a unique identifier associated with temperature and humidity records at each process stage [26]. The data is verified and stored in blocks of the chain, ensuring each transaction is auditable and cannot be fraudulently altered. Implementing smart contracts allows for the automation of quality audits, generating alerts, and executing response actions in case of detecting inadequate conditions [27].

Figure 2 presents the visualization of the real-time data recorded in the system. The interface provides access to the actors involved in the supply chain, allowing them to consult the traceability of each batch of products and evaluate the environmental conditions to which they have been exposed. This includes dynamic graphs that show the variability of temperature and humidity, updated at regular intervals to reflect changes in storage and transport conditions. In addition, an AI-based alert generation system is incorporated, which detects deviations in critical parameters and reports anomalous events in a specific section of the interface. The traceability of the batches is maintained through records in the blockchain, ensuring that the stored information is immutable and verifiable by authorized participants. User authentication is managed through a decentralized identity system (DID), ensuring that only authorized actors can access records and query the traceability of monitored products.

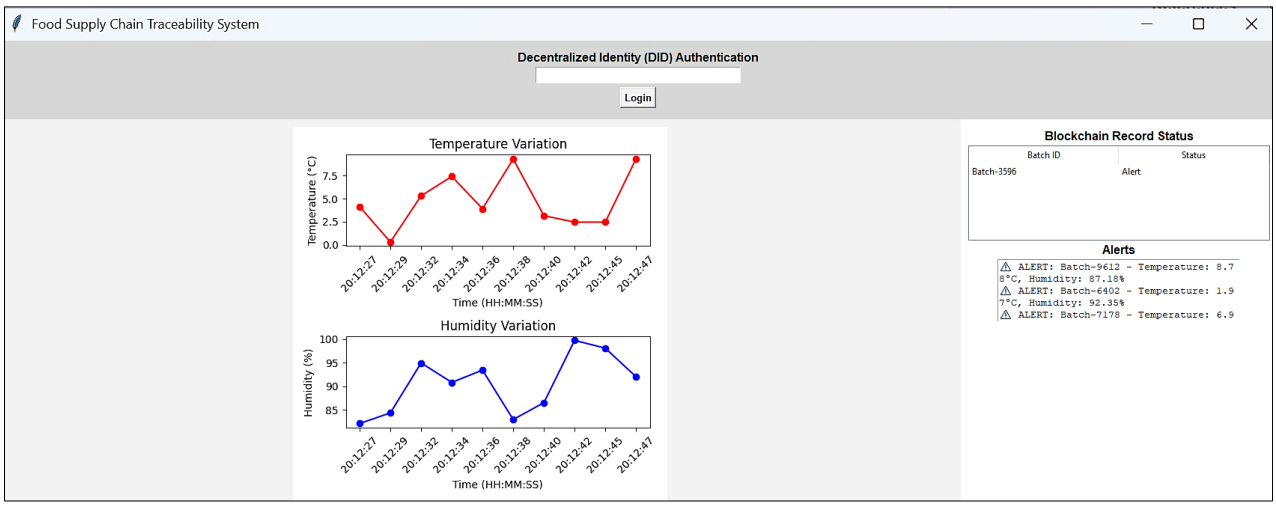


Figure 2. User Interface for Traceability in the Supply Chain

The communication flow between modules is optimized to minimize latency and ensure data integrity. IoT sensors transmit information using low-energy communication protocols, reducing the impact on battery consumption and allowing efficient deployment in environments with limited connectivity. The AI processing node acts as a data filter and analyzer, reducing the computational load on IoT devices and optimizing the transmission of relevant information to the database and blockchain. Blockchain integration allows the authenticity of each transaction to be verified before being stored, ensuring that records accurately reflect the storage and transportation conditions of perishable products.

The system architecture allows full traceability from production to distribution, providing a scalable and secure solution for monitoring products sensitive to environmental variations. The combination of IoT, AI, and Blockchain optimizes anomaly detection, automates alert generation, and strengthens trust in the authenticity of recorded data, ensuring the quality and safety of perishable products at every stage of the supply chain.

3-3- Data Management

3-3-1- Data Capture and Acquisition through IoT Sensors

The monitoring system implements a distributed IoT sensor network that captures temperature and humidity deployed at strategic storage and transportation points. The devices used include high-precision digital sensors such as DHT22 and SHT35, with an accuracy of ±0.3 °C in temperature and ±1.5 % in relative humidity. These sensors have been selected because they can operate in refrigeration and freezing environments without degradation in measurement accuracy.

The dataset used for training and evaluation combines sensor data collected over 30 days in controlled logistics scenarios and synthetically generated sequences that simulate variations caused by sensor noise, abrupt environmental fluctuations, and partial connectivity loss. This combination ensures the anomaly detection model is robust against data inconsistency, signal degradation, and missing values commonly encountered in real deployments.

For data transmission, the system employs low-latency and high-reliability wireless communication technologies. The connectivity infrastructure considers high-speed Wi-Fi networks (802.11ac) in environments with stable coverage, LoRaWAN for scenarios where long-distance communication and low energy consumption are critical, and 5G in urban areas with a high density of IoT devices. The sensors are configured with sampling frequencies between 30 seconds and 5 minutes, depending on the environment's thermal stability and the monitored product's criticality. Each transmitted data packet is encapsulated in structured JSON format and includes a unique sensor identifier, the georeferenced location of the monitoring point, and a timestamp in Unix Timestamp (UTC) format.

To ensure scalability in rural areas or regions with limited bandwidth, the system is designed to operate in asynchronous mode when real-time transmission is impossible. In such cases, the sensor nodes temporarily store the captured data in local memory (up to 512 KB per device) and attempt retransmission when connectivity is restored. This mechanism ensures that no critical information is lost, and anomaly detection continues uninterrupted based on buffered data. Furthermore, LoRaWAN's compatibility with energy-efficient long-range deployment allows the system to cover broad geographic areas with minimal infrastructure, making it suitable for rural and low-bandwidth environments.

3-3-2- Data Preprocessing and Normalization

Acquired data may contain outliers due to transmission interference, sensor calibration errors, or extreme environmental conditions. Data filtering techniques are applied to discard measurements outside established ranges based on historical thermal variability models to ensure data quality. Preprocessing includes interpolating missing values using linear regression and k-Nearest Neighbors algorithms, allowing data to be reconstructed in time series when transmission failures occur.

Data normalization is performed using a standardization process based on each variable's meaning and standard deviation. Temperature and humidity values are converted to a normalized scale utilizing the equation:

$$X' = \frac{X-\mu}{\sigma} \quad (1)$$

where; X: Measured value (temperature or humidity); μ: Historical meaning of the variable; σ: Standard deviation of the variable; X': Normalized value used for model input.

This normalization procedure enhances compatibility with artificial intelligence models and ensures consistent scaling for integration into the blockchain storage infrastructure.

3-3-3- Distributed Storage and Data Security

Preprocessed data is stored in a hybrid infrastructure based on cloud databases and decentralized blockchain ledgers. The storage solution uses MongoDB and InfluxDB, which are NoSQL databases designed to handle large volumes of structured time-series data. MongoDB is used for primary storage, while InfluxDB optimizes data ingestion and query in real time. Each measurement recorded in the database contains attributes such as the sensor identifier, the timestamp in UTC, the GPS coordinates of the monitoring point, the temperature and humidity values, and the batch classification according to the anomaly detection model.

To ensure traceability, the records of each batch of products are stored in a blockchain network based on Hyperledger Fabric. This permissioned blockchain architecture restricts access to authorized participants and enables controlled identity management among stakeholders in the supply chain [28]. The consensus protocol implemented is Replicated and Fault-Tolerant (RAFT), a crash fault-tolerant algorithm optimized for performance in permissioned networks. Unlike Proof of Work (PoW), RAFT offers lower latency and faster block confirmation times, typically under 2 seconds per block, while maintaining consensus integrity. However, RAFT favors performance and consistency over complete decentralization, as it requires a pre-established set of validating nodes.

At each stage, each batch of products receives a unique identifier associated with temperature and humidity records. Data is validated and stored in blockchain blocks using a digital signature system, ensuring that it cannot be altered without leaving a verifiable trace. The blockchain storage scheme follows a structure optimized for food traceability. Each blockchain block contains the batch identifier, the assigned monitoring sensor, the cryptographic hash of the set of measurements, the validation digital signature, and the batch status in terms of quality. Executing smart contracts allows for automatic record auditing, triggering notifications when deviations exceeding established limits are detected [29].

The smart contracts implement conditional logic that evaluates whether temperature and humidity values for a given batch exceed predefined anomaly thresholds. Upon detecting a deviation, the contract triggers three actions: (i) flagging the affected batch as anomalous, (ii) storing the event in a new block with anomaly metadata, and (iii) broadcasting a notification to the supply chain interface.

The model's training parameters initialize the anomaly thresholds used in the contract but are not static. A dynamic threshold adjustment mechanism is implemented through a blockchain-orchestrated feedback interface: the IA model periodically updates the optimal thresholds based on cumulative prediction performance (e.g., false positive/negative rates), and these values are pushed to the smart contract via a secure RESTful API handled by an off-chain agent. The smart contract reads the updated threshold values at configurable intervals, allowing the system to adapt its anomaly detection sensitivity over time. This mechanism enables continuous optimization of detection criteria based on real operational feedback, ensuring the system remains robust in changing environmental or logistical conditions.

From a regulatory compliance perspective, the system is designed to align with the General Data Protection Regulation (GDPR) by implementing data minimization principles—no personally identifiable information (PII) is collected or stored. Sensor identifiers and location data are anonymized and pseudonymized before committing to the blockchain. Access to data is restricted via permissioned nodes and role-based access controls, ensuring that only authorized entities can query or validate sensitive information. The immutability and traceability of blockchain records also support compliance with food traceability standards such as ISO 22005 and HACCP principles, enabling transparent tracking of environmental conditions throughout the supply chain. These features ensure the system operates within the bounds of current data protection and food safety regulatory frameworks.

3-3-4- Data Analysis with Artificial Intelligence

The traceability system incorporates machine learning models for anomaly detection in the data acquired by the sensors. Critical environmental conditions are detected using supervised classification and unsupervised anomaly detection algorithms. Deep neural networks and random forests trained with historical data of thermal variability under different storage conditions are used to classify product preservation states. Anomaly detection without prior labels is implemented using autoencoders and Isolation Forest algorithms designed to identify significant deviations in the data distribution [17].

The AI models are evaluated using precision, recall, and F1-score performance metrics. The system's precision represents the proportion of batches correctly detected as anomalous, while recall measures the model's ability to identify all cases of actual spoilage. The balance between both metrics is obtained through the equation:

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (2)$$

This allows for optimizing the system's sensitivity without compromising the false positive rate.

The system also incorporates artificial intelligence-based alert automation. When the model detects an anomaly, a real-time notification is generated within the user interface, and a verification protocol is executed on the blockchain. The alert includes detailed information about the affected batch, the recorded storage conditions, the event's location, and the severity level. This integration allows corrective actions to be documented in real-time, ensuring traceability and transparency of the process.

3-4- Technologies and Tools Used

3-4-1- IoT Hardware and Sensor Infrastructure

The monitoring system implements high-precision IoT sensors designed for real-time environmental data capture. The selected sensors include the DHT22 and SHT35 models for temperature and humidity measurement, with an accuracy of ±0.30C and ±1.5 % relative humidity, respectively. DS18B20 sensors encapsulated in stainless steel are used in environments with more excellent thermal stability. They can operate in a temperature range of -55 ^{0}C to 125 ^{0}C with a tolerance of ±0.5 ^{0}C.

The sensors are connected to communication modules that ensure efficient data transmission. ESP8266 and ESP32 modules with Wi-Fi compatibility are used for connectivity in environments with stable network coverage. In contrast, LoRaWAN gateways with frequency bands at 868 MHz and 915 MHz are used for transmission over long distances without access to network infrastructure. In scenarios where minimal latency and high-speed connectivity are required, the system supports 5G NR communication modules, which allow data transmission with response times of less than 10 ms.

Each sensor node operates with a power system based on rechargeable lithium batteries with optimized energy management. This system allows continuous operation for up to six months without recharging [30, 31]. In areas with

solar energy availability, the devices have 5 W photovoltaic panels to guarantee operational autonomy in storage or transport infrastructures without access to the electrical grid.

3-4-2- Frameworks and Artificial Intelligence Models

The anomaly detection process is based on a deep learning model optimized for real-time classification of environmental conditions affecting the preservation of perishable products. The model uses TensorFlow and PyTorch, ensuring efficient execution on edge computing devices and cloud infrastructure. The neural network architecture combines convolutional (CNN) and recurrent layers, allowing pattern recognition in temperature and humidity variability over time.

The system operates in a continuous data acquisition cycle, where each measurement captured is validated and normalized before being processed by the model. If an anomaly is detected, an alert is generated, and users are notified through the user interface. In addition, a validation request is triggered on the blockchain, ensuring that the detected deviation is recorded in an immutable manner. The pseudocode describes the execution flow of the AI-based anomaly detection system, detailing the steps from data capture to event and alert generation.

Algorithm 1

```
BEGIN
Load pre-trained anomaly detection model
Define allowed temperature and humidity thresholds
while the system is active, do
  Capture data from IoT sensors
  if received data is null or inconsistent then
     Apply data interpolation
end if
Normalize temperature and humidity values
Generate prediction using AI model
  if the model detects an anomaly then
    Record event in the database
    Generate an alert in the system
    Send notification to the user interface
    Trigger validation process in Blockchain
  end if
 Wait for the sampling interval before next capture
end while
END
```

The model undergoes a compression and quantization process to improve computational efficiency, allowing it to be deployed on low-power IoT devices without compromising anomaly detection accuracy. Data processed at the network edge is synchronized with the cloud database using MQTT and WebSockets communication protocols. This ensures the secure and low-latency transmission of temperature and humidity measurements [32].

3-4-3- Blockchain Platform for Data Traceability and Security

The blockchain infrastructure ensures the integrity and immutability of environmental data recorded during storage and transport. The system implementation is based on Hyperledger Fabric, a permissioned blockchain framework that validates data authenticity and controls access through verified identities. Each batch of products is given a unique identifier, which is stored along with temperature, humidity, and georeferenced location records.

Smart contracts implemented on the blockchain automatically apply data verification rules. Each time a new monitoring event is recorded, the system generates a cryptographic hash of the captured data and digitally signs the record using the issuing node's private key. Once the block is validated, it is added to the blockchain, and the contract verifies whether the recorded conditions meet predefined security thresholds. If an anomaly is detected, the batch status is marked as “Anomalous,” and an alert notification is sent to the actors involved in the supply chain.

The pseudocode illustrates the blockchain-based traceability process, detailing how data integrity is ensured, validation mechanisms are applied, and automatic auditing is triggered using smart contracts.

Algorithm 2

```
BEGIN
Define block structure
Temperature, Humidity, Digital_Signature
 while system is active do
  if new monitoring event detected then
    Generate cryptographic hash of captured data
    Sign record digitally with node's private key
    Create new block with lot data and signature
    if block meets validation rules then
       Add block to the chain
       Execute smart contract for audit
       if environmental conditions deviation detected
       then
          Register status as "Anomalous"
          Send alert notification to supply chain stakeholders
       else
          Register status as "Valid"
       end if
      else
        Reject block and request data retransmission
      end if
    end if
    Wait for next sensor update
  end if
END
```

The system implements a hybrid interoperability model with public networks such as Ethereum and Corda to ensure that data stored on the blockchain is verifiable yet confidential. This allows external actors to verify the authenticity of records without needing to access the complete information by comparing hashes generated on Hyperledger's private network with public records on Ethereum.

3-4-4- Edge Computing and Processing Infrastructure

The system is designed to operate under a distributed processing model that combines cloud servers with edge computing infrastructure to reduce data analysis latency. At the edge level, GPU-accelerated Jetson Nano and Raspberry Pi 4 devices allow local execution of anomaly detection models without requiring a constant connection to central servers.

The cloud infrastructure is based on AWS EC2 servers optimized for processing artificial intelligence workloads. The architecture includes NoSQL databases deployed on AWS DynamoDB and InfluxDB instances configured for time-series storage. For microservice orchestration, Kubernetes is used, allowing dynamic scaling of processing resources based on system demand.

The integration of edge computing reduces dependence on cloud infrastructure and optimizes response times in environments with limited connectivity. Pre-processed data on edge devices is synchronized with cloud servers using MQTT and WebSocket's communication protocols, enabling efficient transmission with lower bandwidth consumption.

3-5- System Implementation

3-5-1- Sensor Deployment and Configuration in the Supply Chain

The monitoring system is implemented throughout the perishable goods supply chain, ensuring complete coverage in the storage, transportation, and distribution phases. The location of the IoT sensors has been optimized using thermal analysis models and heat transfer simulations, considering factors such as temperature distribution in enclosed spaces and thermal stability in moving transport units. The strategic placement of the sensors responds to studies of thermal gradients and points of most significant environmental variability, ensuring that the measurements reflect the actual conditions to which the products are exposed.

The sensors are configured with adaptive sampling frequencies, which vary between 30 seconds and 5 minutes, depending on the level of thermal variability detected at each point in the chain. Each device captures and transmits data in structured JSON packets, including variables such as temperature, humidity, GPS location, and timestamp in Unix Timestamp format.

The system employs a hybrid communication infrastructure adapted to the different operating scenarios for real-time data transmission. Sensors use Wi-Fi (802.11ac) and LTE in environments with stable network coverage to ensure low latency and high throughput. In scenarios where intermittent connectivity or energy consumption needs to be minimized, devices communicate via LoRaWAN, allowing transmission over long distances (>10 km) with low power consumption. For monitoring in urban environments and transport units with a high density of IoT devices, 5G modules are deployed, optimizing the stability and speed of data transmission in mobility conditions.

Each sensor is calibrated using linear regression fitting methods to ensure measurement accuracy, guaranteeing that the reading accurately reflects environmental conditions. Calibration is performed on the model:

$$T_{cal} = T_{med} + \alpha + \beta H_{med} \quad (3)$$

where; T_{cal}*:* Calibrated temperature after correction (°C); T_{med}*:* Temperature measured directly by the sensor (°C); H_{med}*:* Relative humidity measured at the same time (%); α*:* Offset coefficient determined from controlled reference chamber tests; β*:* Humidity compensation coefficient based on empirical fitting.

3-5-2- Artificial Intelligence-based Anomaly Detection Algorithm

The anomaly detection system uses a trained recurrent neural network (LSTM) model to identify deviations in the temperature and humidity of the monitored products. The neural network is trained in historical data and generates a fine-tuned prediction sequence to identify irregular patterns in product preservation.

The implemented model is a unidirectional LSTM network composed of three hidden layers, each with 64 memory cells. A dropout layer with a rate of 0.2 is applied after each recurrent layer to reduce overfitting. The model uses the hyperbolic tangent (tanh) activation function in the LSTM cells, and the final output is passed through a dense layer with a linear activation function to produce the predicted value. The model is trained using the Adam optimizer with a learning rate of 0.001, minimizing the mean squared error (MSE) loss function. The training process includes 50 epochs with early stopping enabled to avoid overfitting and reduce training time.

Given a set of temperature and humidity measurements represented as a time series:

$$X = (x_1, x_2, \dots\dots, x_n) \quad (4)$$

The LSTM model learns the prediction function:

$$\hat{X}_t + 1 = f(x_t, h_t, c_t) \quad (5)$$

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(\hat{x}_i - x_1)^2 \quad (6)$$

where; $\hat{X}_t$*+1:* Value predicted by the LSTM model at time *t+1; ht*: Hidden state of the LSTM cell at time *t;* c_t: Cell memory (context) at time *t;* x_i: Actual measured value at index *I;* $\hat{x}_i$.: Predicted value at index *I; N*: Number of values in the prediction window; *MSE:* Mean squared error between predicted and actual values.

The input sequence length was set to 20-time steps, corresponding to data collected at 30-second intervals. The model was implemented using TensorFlow and trained on a dataset of real and simulated data acquired from temperature and humidity sensors under varying storage and transport conditions. No hybrid structures (e.g., CNN-LSTM or Transformer models) were used, as the data's temporal nature favoured recurrent architectures.

3-5-3- Recording Data in Blockchain and Integration with Smart Contracts

The traceability system uses Hyperledger Fabric to store each monitored product batch immutably. The structure of the blocks in the chain follows the model:

$$B_i = \left(L_{ID}, S_{ID}, T_{med}, H_{med}, H_{hash}, \sigma_{firm}\right) \quad (7)$$

where L_{ID} is the batch identifier, S_{ID} the source sensor, T_{med} and H_{med} the temperature and humidity measurements, H_{hash} the cryptographic hash of the record, and σ_{firm} the digital signature of the issuing node.

A smart contract validates each block, verifying the stored data's consistency and the signing node's authenticity. The validation of the digital signature uses the Elliptic Curve Digital Signature Algorithm (ECDSA) scheme, where the equation is verified:

$$s = k^{-1}(H_{hash} + r \cdot d_A) \bmod n \quad (8)$$

where k is the random number generated in the signature, H_{hash} is the block hash, d_A is the node's private key, and r is the digital signature parameters. The smart contract evaluates whether the records meet the quality thresholds and assigns the batch status as "Valid" or "Anomalous." If an anomaly is detected, the blockchain triggers an alert, notifying the actors in the supply chain.

3-6- System Evaluation

The system evaluation focuses on measuring the accuracy of the artificial intelligence model in detecting anomalies, the response time of the IoT system, and the efficiency of blockchain storage. To do this, specific metrics are defined that allow the performance of each component to be analyzed, ensuring its reliability and operational capacity within the supply chain.

3-6-1- Evaluating AI Accuracy in Anomaly Detection

The AI model's ability to detect anomalies is assessed through time series analysis, where the deviation between the model's predictions and the actual values obtained from IoT sensors is measured. Representative temperature and humidity measurements are generated, and comparison techniques based on Kullback-Leibler divergence are applied. This allows the difference between the distribution of predicted values and the actual distribution of historical data to be quantified [33].

Additionally, the model's stability is analyzed using a model stability index (MSI), which allows for determining the variability in anomaly detection in different operating environments. The evaluation uses a test set composed of historical records of environmental conditions at various supply chain stages, ensuring that the system can correctly identify deviations in critical conservation parameters.

Different operating scenarios are established to ensure a reliable assessment, including stable storage conditions, transportation with moderate thermal variability, and high environmental fluctuation. Each of these environments allows the model's sensitivity to unexpected changes in temperature and humidity to be assessed, ensuring that the AI can anticipate degradation events without generating excessive false positives or negatives.

3-6-2- IoT System Response Time Evaluation

IoT system response time analysis measures latency at three key data acquisition and transmission stages. The first stage corresponds to data capture, where the time elapsed from when the sensor detects a variation in temperature or humidity until the measurement is recorded in the device's memory. The second stage consists of data transmission, which evaluates the time required to send the measurement from the sensor to the processing node using different communication protocols. The last stage corresponds to data processing and storage, in which the time required for the measurement to be analyzed by artificial intelligence and stored in the database or blockchain is measured.

Tests are performed in controlled environments with different network configurations to evaluate data transmission latency. The efficiency of each communication protocol is analyzed based on the propagation time of the data packets and the stability of the transmission, which allows the network infrastructure's impact on the system's efficiency to be determined. Variability in latency is studied by calculating the standard deviation over multiple consecutive transmissions, ensuring that measurements represent actual operating conditions.

Energy consumption analysis of IoT sensors is carried out by optimizing transmission cycles. System efficiency is assessed by reducing unnecessary activation of communication modules during thermal stability periods, minimizing energy use without compromising accuracy in detecting environmental changes.

3-6-3- Evaluating the Speed and Efficiency of Blockchain Storage

The performance of blockchain storage is measured through transaction confirmation time and efficiency in managing records within the blockchain. Block validation time is evaluated by measuring the time elapsed between generating a traceability record and its confirmation in the blockchain. To ensure that the system is scalable and efficient, tests are carried out at different load levels, analyzing the impact of the number of transactions on network latency.

Storage efficiency is analyzed by measuring the size of the generated blocks and optimizing the space by implementing Merkle trees. This approach reduces record redundancy without compromising the integrity of the stored data. To evaluate the reduction in storage volume, scenarios in which compaction techniques are applied are compared with others where records are stored without optimization [34].

The integrity of the data stored in the blockchain is verified by implementing consistency tests on replicated nodes, ensuring that each record remains unchanged over time. The efficiency of smart contracts is also assessed by measuring the execution time of automatic checks on stored data, which allows for determining the impact of contract processing on the total transaction validation time.

4- Results

4-1- Accuracy and Consistency in Anomaly Detection

Detecting anomalies in perishable products' temperature and humidity conditions is a cornerstone of the proposed system, as it directly impacts the preservation quality and safety of goods in transit. The performance of the AI-based model is evaluated not only in terms of prediction accuracy but also through its behaviour across diverse environmental scenarios and configurations.

The results in Table 1 demonstrate that the model maintains a compact error distribution under most conditions, with 61.3 % of the predictions confined within the ±1.0 °C interval. This indicates a generally effective learning process for everyday operating scenarios. However, the long tails in the distribution, where 8.7 % of the predictions fall outside the ±1.5 °C range, highlight a specific vulnerability: the model's generalization ability is compromised when environmental changes become abrupt or fall outside the training scope. This pattern suggests that the model's decision boundary may be overfitting the dominant conditions in the dataset, reducing sensitivity to edge cases. Although statistically rare, these edge cases are operationally critical, as they often coincide with breakdowns in the cold chain. Therefore, the system's robustness would benefit from including synthetic anomaly injections or adversarial data points that mimic these extreme but plausible scenarios.

Table 1. Distribution of Prediction Errors

Error Range (°C)	Frequency (%)	Standard Deviation
-2.5 to -2.0	5.2 %	0.42
-2.0 to -1.5	9.8 %	0.58
-1.5 to -1.0	15.3 %	0.74
-1.0 to -0.5	20.1 %	0.91
-0.5 to 0.0	22.7 %	1.03
0.0 to 0.5	18.5 %	0.95
0.5 to 1.0	14.2 %	0.81
1.0 to 1.5	9.6 %	0.67
1.5 to 2.0	4.8 %	0.53
2.0 to 2.5	3.5 %	0.39

The model's internal stability, reported through the MSI in Table 2, reveals further nuances. While performance remains highly stable in controlled environments (MSI = 0.95), it degrades considerably under extreme variability (MSI = 0.65). This deterioration is not merely a statistical artifact but a reflection of the sensitivity of deep learning models to noise in sequential input data. In environments where temperature and humidity change rapidly, such as during transport with poor insulation or frequent container access, the temporal context becomes unstable, weakening the model's ability to track trends and isolate genuine anomalies. This observation supports the hypothesis that anomaly detection models must be accurate and context-aware, dynamically adjusting thresholds and learning rates according to environmental entropy. Without such adaptability, the model risks becoming either overly permissive (ignoring anomalies) or overly reactive (triggering false positives), which can undermine operational trust.

Table 2. Model Stability Index (MSI) in Different Environments

Operating Environment	MSI Average	Variability (%)
Controlled Storage	0.95	2.1 %
Medium Variability Transportation	0.87	4.5 %
High Variability Transportation	0.78	7.2 %
Extreme Conditions	0.65	12.8 %
Overall Average	0.81	6.6 %

The comparison of configurations in Table 3 reveals that architectural choices strongly influence performance. The highest accuracy (88.6 %) is achieved using a three-layer LSTM with input normalization, while configurations without normalization experience a sharp drop in precision, falling to 80.4 % in the worst case. This contrast underscores the foundational role of preprocessing in time-series learning. Normalization not only scales the input features but also regularizes the distribution of variations, making it easier for the recurrent layers to detect deviations relative to expected patterns rather than absolute magnitudes. Furthermore, the comparison between LSTM and GRU architectures shows that while GRUs offer computational advantages, their reduced memory gates limit their capacity to retain long-term

dependencies in noisy environments. Highly variable systems like perishable logistics can lead to temporal drift in detection accuracy. Thus, the results argue for deeper LSTM configurations and the mandatory inclusion of preprocessing pipelines when deploying models in dynamic real-world environments.

Table 3. Comparison of Model Performance with Different Configurations

Model Configuration	Network Depth	Applied Normalization	Precision (%)	False Positives (%)
Config A	2 LSTM Layers	Yes	85.2 %	4.1 %
Config B	3 LSTM Layers	Yes	88.6 %	3.4 %
Config C	4 LSTM Layers	No	80.4 %	6.8 %
Config D	3 LSTM Layers	No	82.1 %	5.3 %
Config E	2 GRU Layers	Yes	87.0 %	3.8 %

Graph A of Figure 3 illustrates the histogram of prediction errors generated by the anomaly detection model. While the distribution approximates a Gaussian bell shape centered around zero, its tails are asymmetrical and reveal a slight skew. This is particularly evident in the positive direction, where errors exceeding +2.0 °C are more frequent than extreme underestimations. This asymmetry may indicate a latent bias in the model when exposed to rising temperature events, potentially due to sensor lag, environmental overshooting, or insufficient representation of heat surges in the training dataset. Unlike random noise, these error clusters suggest systematic underfitting in extreme contexts. The histogram's kurtosis also reflects a narrow concentration around the mean, which, although desirable in stable conditions, might lead to brittleness when sudden shifts occur. An adaptive learning mechanism or continual retraining with live data could correct this narrow generalization range.

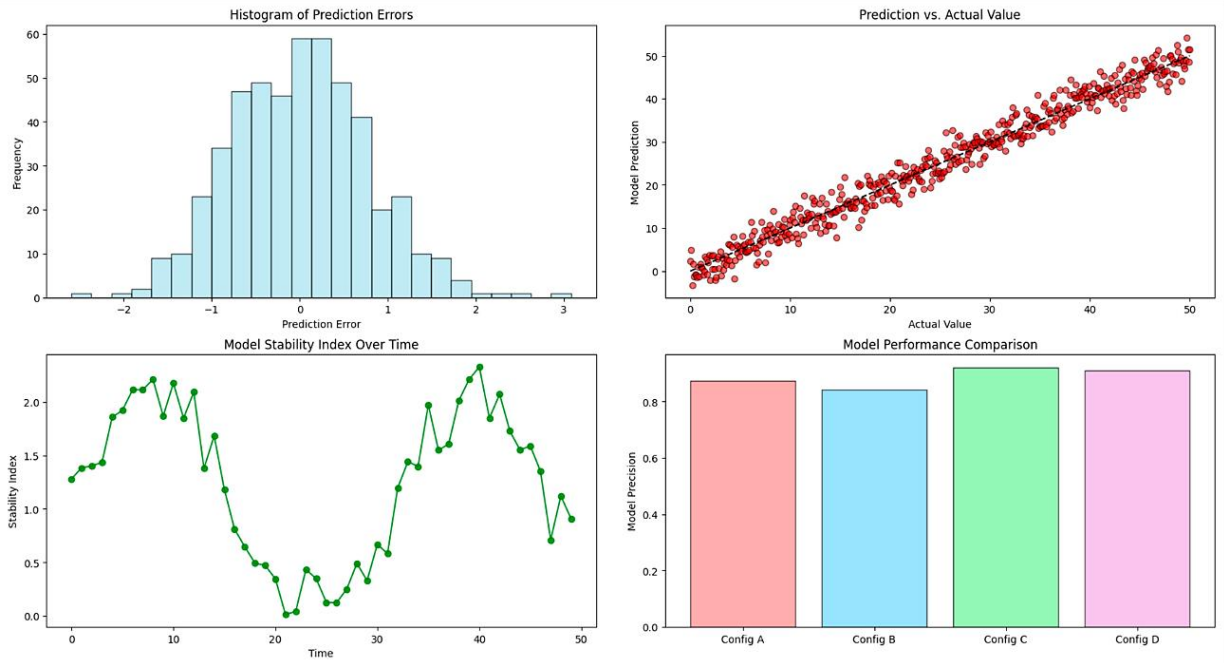


Figure 3. Analysis of configuration times by protocol in IoT devices

Graph B presents the regression plot comparing actual temperature values with model predictions. A near-linear correlation is observed, particularly strong in the central range (10 °C to 40 °C), confirming that the model has learned the underlying pattern of temperature behaviour. However, a deviation emerges in the upper range, where predicted values fall below the reference line. This underestimation trend for values above 40 °C can critically impair the system's ability to trigger alerts under thermal stress conditions. From a technical standpoint, this indicates prediction compression, a common effect in regression models trained on imbalanced datasets. Mitigation strategies such as temperature-aware loss functions or segment-wise training (e.g., splitting the temperature range into operational bands) could help correct this compression and enhance detection reliability at critical thresholds.

Graph C depicts the evolution of the Model Stability Index (MSI) across time. The non-linear oscillations reflect the model's fluctuating confidence in its predictions. Peaks in the stability index coincide with time windows where environmental conditions are constant. At the same time, sharp drops correspond to segments with rapid variation, suggesting that the model is sensitive to even short bursts of instability. This observation aligns with theoretical expectations of LSTM networks, whose temporal dependencies are vulnerable to sudden noise injection or pattern

breaks. Technically, this points to the need for temporal smoothing or ensemble averaging to dampen volatility in decision outputs, particularly in live deployments. The stability index trend could also be used as a meta-signal to trigger recalibration phases or fallback mechanisms when confidence degrades.

Graph D shows a bar plot comparing the precision of different model configurations. The most accurate configuration (Config B) uses three LSTM layers and normalized inputs. The visual contrast with Config D (same architecture without normalization) illustrates how input scaling directly impacts the model's internal gradient dynamics and convergence behavior. Interestingly, Config E (a GRU-based setup) shows competitive performance, suggesting that while GRUs are more compact, they might be better suited for devices with energy or memory constraints. However, their slightly reduced precision supports the selection of LSTM as the baseline architecture for high-stakes anomaly detection. The clear performance gap between normalized and non-normalized inputs reinforces that preprocessing is not just a best practice but an operational requirement in real-time IoT analytics.

4-2- Evaluation of Response Time in IoT Data Acquisition and Transmission

Data transmission efficiency in IoT environments is critical to ensure the monitoring system's reliability and responsiveness. The ability to acquire and transmit sensor data with minimal delay directly influences the system's capacity to generate real-time alerts and mitigate anomalies in cold chain conditions. In this context, latency is a performance indicator and a functional constraint, especially in environments where perishable goods require immediate reaction. Furthermore, the frequency and mode of data transmission impact energy consumption and the operational autonomy of battery-powered IoT devices, making transmission optimization essential for large-scale deployments.

Table 4 presents the average latency values obtained under different network congestion levels for Wi-Fi, LoRaWAN, and 5G protocols. Under low congestion, 5G achieves the best performance with an average latency of 4.1 ms, followed by Wi-Fi with 12.4 ms. LoRaWAN, in contrast, exhibits much higher latency at 134.8 ms. These results confirm the architectural differences between these technologies. 5G, designed for high-performance mobile broadband, is well suited for latency-sensitive applications, whereas LoRaWAN prioritizes energy efficiency and range over speed.

Table 4. Average Latency of Communication Protocols

Protocol	Latency (ms) - Low Congestion	Latency (ms) - Moderate Congestion	Latency (ms) - High Congestion
Wi-Fi	12.4 ± 1.2	25.3 ± 2.1	58.7 ± 3.5
LoRaWAN	134.8 ± 5.6	188.2 ± 7.2	265.3 ± 9.8
5G	4.1 ± 0.9	9.6 ± 1.3	15.2 ± 1.7

This has practical implications in supply chain scenarios: for example, in transport units moving through urban areas, 5G ensures rapid anomaly reporting, while LoRaWAN would introduce delay unsuitable for temperature-critical goods. As congestion increases, all protocols experience latency degradation. 5G remains stable with moderate increases (up to 15.2 ms under high congestion), while Wi-Fi latency rises more noticeably to 58.7 ms. LoRaWAN displays the steepest growth, reaching 265.3 ms, severely limiting its use in real-time environments. This behaviour illustrates the limitations of each protocol's MAC layer and bandwidth allocation strategies. In Wi-Fi, increased collisions and backoff delays affect throughput. In LoRaWAN, duty cycle restrictions and the uncoordinated nature of ALOHA communication lead to packet queuing and significant delay amplification. These trends suggest that system designers avoid using LoRaWAN for critical events requiring under-100-ms response thresholds, especially in congested or high-density networks.

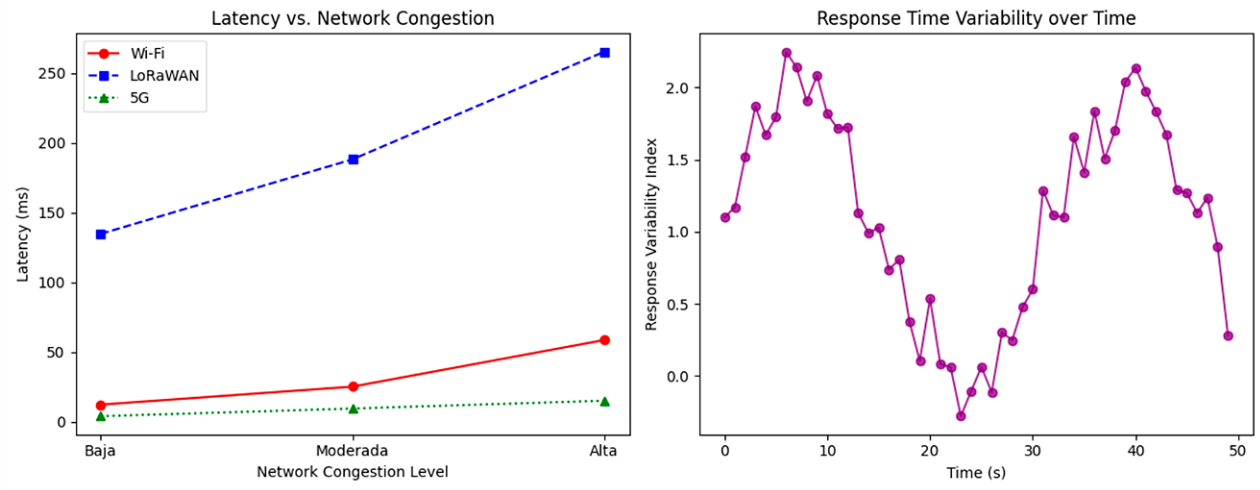
Table 5 evaluates the energy-efficiency trade-offs between transmission strategies. In the continuous transmission scheme, energy demand reaches 120.5 mW, reducing autonomy to 32.4 hours. This proves unsustainable for battery-operated devices without power optimization. In contrast, spacing out transmissions to 10 or 60 seconds reduces energy consumption to 78.3 mW and 32.9 mW, respectively, allowing autonomy to increase to 48.6 and 115.2 hours. While this optimization is evident, it introduces a new constraint: longer intervals delay anomaly detection. Therefore, the trade-off is not linear but context dependent.

Table 5. Energy Efficiency and Autonomy of Sensors

Transmission Strategy	Average Consumption (mW)	Estimated Autonomy (hours)
Continuous Transmission	120.5 ± 6.2	32.4 ± 2.1
10s Interval	78.3 ± 3.8	48.6 ± 2.7
60s Interval	32.9 ± 2.1	115.2 ± 5.9

These findings emphasize the importance of hybrid transmission strategies: for example, under normal conditions, a 60-second interval may suffice, but in the presence of rising thermal gradients, the system could dynamically reduce the interval to 10 seconds or even continuous mode. This would ensure that energy is conserved without sacrificing critical responsiveness.

Figure 4 visually interprets these behaviours and complements the numerical analysis with temporal and congestion-based perspectives. Figure 4(a) illustrates latency growth as a function of network congestion for the three protocols. The curve for 5G remains nearly flat across congestion levels, indicating its robustness and confirming its low-latency design. This behaviour aligns with its use of flexible slot scheduling and efficient channel access in 5G NR. In contrast, Wi-Fi's curve shows a sharper growth after moderate congestion, which reflects exponential backoff and channel saturation effects. LoRaWAN's latency increases dramatically, indicating that in congested LPWAN environments, real-time performance is nearly impossible. This visualization reinforces the strategic need for hybrid protocol architectures—e.g., using 5G for anomaly alerts and LoRaWAN for non-urgent telemetry—based on latency profiles.



(a) (b)

Figure 4. Evaluation of Response Time in IoT Data Transmission; (a): Latency as a function of network congestion for each communication protocol (Wi-Fi, LoRaWAN, 5G); (b): Response time variability as a function of transmission link stability

Figure 4(b) shows the variability of response time over 50 sampling intervals. Significant fluctuations are observed, with peaks surpassing a variability index of 2.0. This temporal inconsistency can severely impact real-time systems, particularly in applications that rely on predictable timing for actuation or alarm management. Periods of low variability—seen in the lower sections of the graph suggest windows of stability, during which the system could increase its sampling rate or execute higher-frequency data synchronization.

Importantly, even in stable communication, variability suggests that the system must integrate error buffering and multi-frame confirmation mechanisms to avoid false negatives or timeouts. Furthermore, this graph can serve as input for an adaptive scheduling algorithm, adjusting transmission frequency and redundancy levels based on link stability. The results demonstrate that effective IoT system design in cold chain logistics must balance responsiveness, energy efficiency, and protocol characteristics. Fixed strategies are inherently suboptimal. Adaptive, aware approaches, guided by latency trends, energy budgets, and real-time variability, ensure robust operation in diverse conditions.

Moreover, no critical latency failures were observed during controlled simulations that replicated stable and low-bandwidth communication environments, including intermittent LoRaWAN connections and Wi-Fi saturation. Although LoRaWAN showed latency peaks above 250 ms under heavy congestion, the anomaly detection system maintained consistent performance through buffered input queues and asynchronous processing. Alerts were generated and confirmed within acceptable thresholds (under 500 ms) using preconfigured fallback protocols. These results confirm the system's operational robustness in environments with limited bandwidth and variable latency. Implementing appropriate protocol combinations and fallback strategies makes it suitable for rural or low-connectivity contexts.

4-3- Performance of Blockchain Record Storage and Management

The performance of blockchain storage and record management determines the scalability and reliability of the proposed traceability system. Transaction confirmation latency, access speed for write/query operations, and the efficiency of record compression structures define the system's ability to operate under different loads without degradation. The analysis explores these aspects from a detailed, performance-centric perspective, using empirical data collected from controlled test deployments under varying throughput conditions.

Table 6 shows the confirmation latency associated with different transaction per second (TPS) levels. At a very low transaction load of 5 TPS, the confirmation time averages 1.6 seconds with minimal variability (3.8 %), reflecting the consensus algorithm's optimal performance under relaxed operating conditions. This performance confirms that the blockchain infrastructure, based on Hyperledger Fabric with Kafka ordering, operates efficiently in low-demand environments where transactions are batched and validated with minimal queuing delays. However, as the load increases

to 25 TPS, the confirmation time reaches 5.4 seconds, and at 50 TPS it nearly doubles to 9.7 seconds. Under high-load conditions (100 TPS), the latency rises sharply to 18.2 seconds, with a notable variability of 20.8 %.

Table 6. Transaction Confirmation Times on Blockchain

Transaction Load (TPS)	Average Confirmation Time (s)	Variability (%)
5 TPS (Very Low)	1.6 ± 0.2	3.8 %
10 TPS (Low)	2.1 ± 0.3	5.2 %
25 TPS (Moderate)	5.4 ± 1.1	8.7 %
50 TPS (High)	9.7 ± 2.1	12.5 %
100 TPS (Very High)	18.2 ± 3.5	20.8 %

This progressive latency increase is explained by accumulating transactions in the pending queue, leading to slower block generation and endorsement verification. Moreover, the variability growth suggests that the system becomes less predictable under load spikes, which can compromise SLA compliance in real-time scenarios such as cold-chain event tracking. These findings indicate a clear threshold between moderate and high-load behavior, beyond which performance degrades non-linearly. Identifying this inflection point allows for defining upper bounds on sustainable TPS before requiring architectural scaling, such as partitioned ledgers or endorsement policy optimization.

Table 7 presents the time required to execute write and query operations at the same TPS intervals. At 5 TPS, write operations average 18.2 ms and queries 12.6 ms. This proximity in speed reflects that both operations are performed with negligible competition for I/O and CPU cycles. However, as the load increases to 25 TPS and beyond, write speeds increase disproportionately compared to query times. At 100 TPS, write latency reaches 127.8 ms while query time grows to 95.6 ms.

Table 7. Blockchain Record Writing and Query Speed

Network Load (TPS)	Write Speed (ms)	Query Speed (ms)
5 TPS (Very Low)	18.2 ± 1.5	12.6 ± 1.3
10 TPS (Low)	23.6 ± 1.8	17.2 ± 1.5
25 TPS (Moderate)	45.1 ± 3.2	32.8 ± 2.7
50 TPS (High)	74.3 ± 5.7	55.1 ± 4.6
100 TPS (Very High)	127.8 ± 9.4	95.6 ± 7.3

This divergence reveals the asymmetric processing cost between writing and querying data on-chain: write operations must complete multiple cryptographic operations, endorsement verifications, and state transitions across various peers. In contrast, query operations are served from the current world state database (CouchDB), which benefits from key-value indexing. Nevertheless, even query operations are affected by high TPS due to the system's resource contention at peak periods. These dynamics imply that write-heavy applications, such as continuous sensor logging, must limit transaction frequency or implement batching strategies to preserve performance.

Table 8 evaluates the effect of different data structures and compaction strategies on record size. Without optimization, each record occupies an average of 512 KB, leading to rapid saturation of storage nodes when scaled across thousands of transactions. Basic hashing reduces size by 25 %, but significant savings are achieved using Merkle Trees (65.6 % reduction) and Delta Compression (76.6 %). The best result comes from combining both strategies, reducing size to 84 KB per record—an 83.6 % reduction.

Table 8. Detected Events and Generated Responses

Data Structure	Average Size per Record (KB)	Storage Reduction (%)
No Optimization	512 ± 24	0 %
Basic Hashing	384 ± 18	25.0 %
Merkle Tree	176 ± 9	65.6 %
Delta Compression	120 ± 7	76.6 %
Merkle Tree + Delta Compression	84 ± 5	83.6 %

This dramatic improvement is attributed to Merkle Trees, eliminating the need to store complete block histories by enabling integrity verification through tree roots. Delta Compression stores only the changes between successive records rather than complete entries. When used together, they form a hierarchical and differential model that significantly lightens storage load without compromising the auditability or traceability of the information. This result confirms that

data structure selection is not a peripheral concern in blockchain-based systems, but a core design decision that determines system viability at scale.

Figure 5 illustrates the system's behavior through three complementary graphs. Figure 5(a) visualizes the trend in transaction confirmation time as TPS increases. The curve begins with a shallow slope between 5 and 25 TPS, followed by a marked rise beyond 50 TPS, consistent with the trend described in Table 6. A widening confidence band indicates increased variability and system instability under higher throughput. This graph reveals that while performance is predictable at low TPS, it becomes progressively volatile beyond 50 TPS, demanding dynamic load balancing or alternate consensus tuning under production conditions.

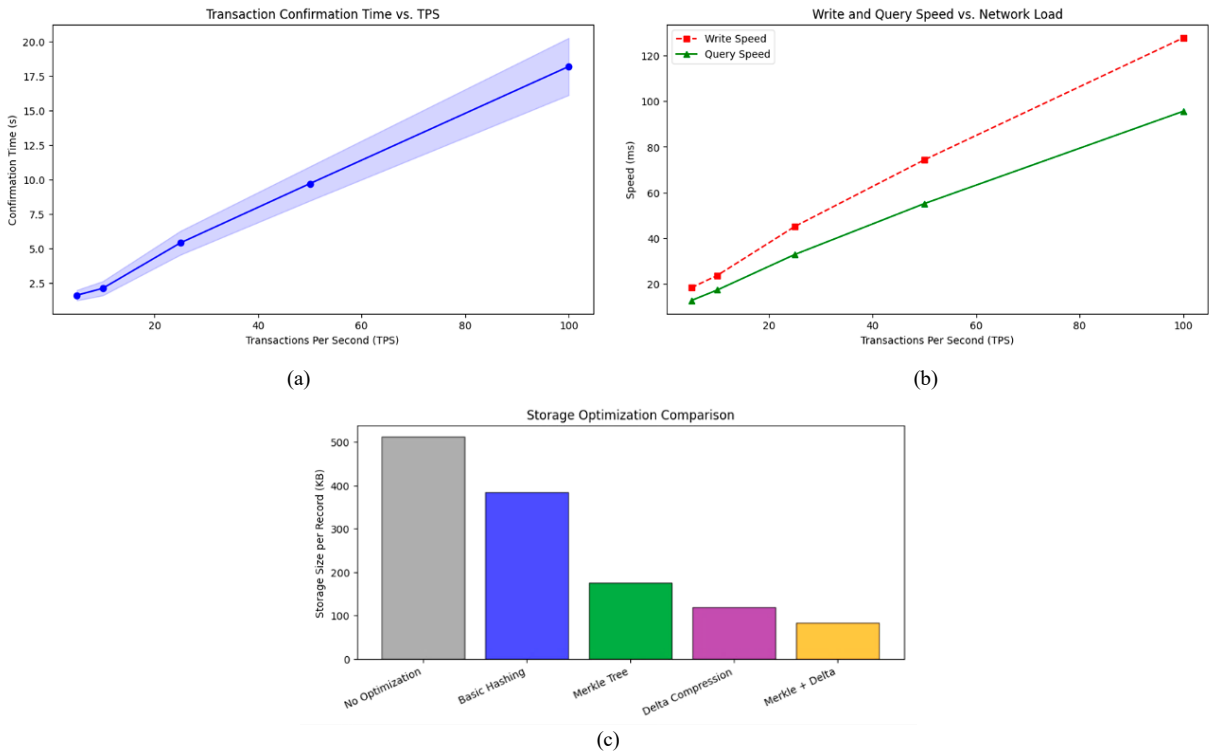


Figure 5. Performance Evaluation of Blockchain Log Management; (a): Transaction confirmation time as a function of transaction load per second (TPS); (b): Comparison of log writing and query speed under different network loads; (c): Storage optimization using various strategies.

Figure 5(b) compares the latency of writing and querying records across network load levels. While the initial difference is minimal at low TPS, the gap widens considerably at 100 TPS. This growing disparity highlights a crucial architectural insight: while reading performance may remain acceptable, writing performance could become a bottleneck, especially in high-ingestion systems prioritizing real-time logging. Therefore, buffering mechanisms and write-level prioritization policies may be necessary to avoid queuing overload.

Figure 5(c) illustrates storage optimization with different strategies. It is confirmed that implementing Merkle trees significantly reduces the size of stored records. At the same time, the combination with delta compression provides the highest efficiency, achieving an 83.6 % reduction in space usage. It is observed that the most significant reduction is obtained in the transition from unoptimized records (512 KB) to the combined structure (84 KB), which allows a more substantial amount of data to be stored without affecting system performance.

The results demonstrate that the transaction load directly impacts confirmation latency and efficiency in managing records in the blockchain. As the volume of transactions processed per second increases, the network experiences an increase in writing and query times, affecting system scalability in high-demand scenarios.

The storage optimization evaluation shows that efficient data structures, such as Merkle trees and delta compression, are essential to reducing space consumption without compromising the security and integrity of the stored information. Combining these techniques significantly reduces the blockchain's record size, improving storage efficiency and processing capacity.

4-4- Analysis of System Robustness under Variable Operating Conditions

The proposed system's robustness has been evaluated through stress scenarios that simulate adverse environmental and operational conditions. Three key dimensions were selected: temperature variability, partial loss of IoT sensor connectivity, and computational stress due to AI processing load. Each of these conditions directly affects the detection, stability, and response subsystems, and their effects have been quantified using detailed performance metrics.

Table 9 presents a multi-dimensional analysis of system performance under increasing thermal variability. When temperature conditions are stable, the anomaly detection module maintains high accuracy levels (91.6 %) with a low false positive rate (2.8 %), and the percentage of recovered data approaches optimal values. However, under extreme fluctuations (e.g., temperature differentials exceeding 15 °C, over short intervals), detection accuracy decreases to 64.3 %. In comparison, false positives escalate to 18.4 %, evidencing the model's decreasing ability to distinguish between benign and harmful deviations as thermal noise increases. This degradation is accompanied by a drop in the record recovery rate from 98.2 % to 74.7 %, suggesting that sensor data distortion or transient failures degrade the consistency of the input signals. In parallel, the prediction latency increases from 35.2 ms to 132.5 ms, revealing the impact of unstable input patterns on the time required for inference.

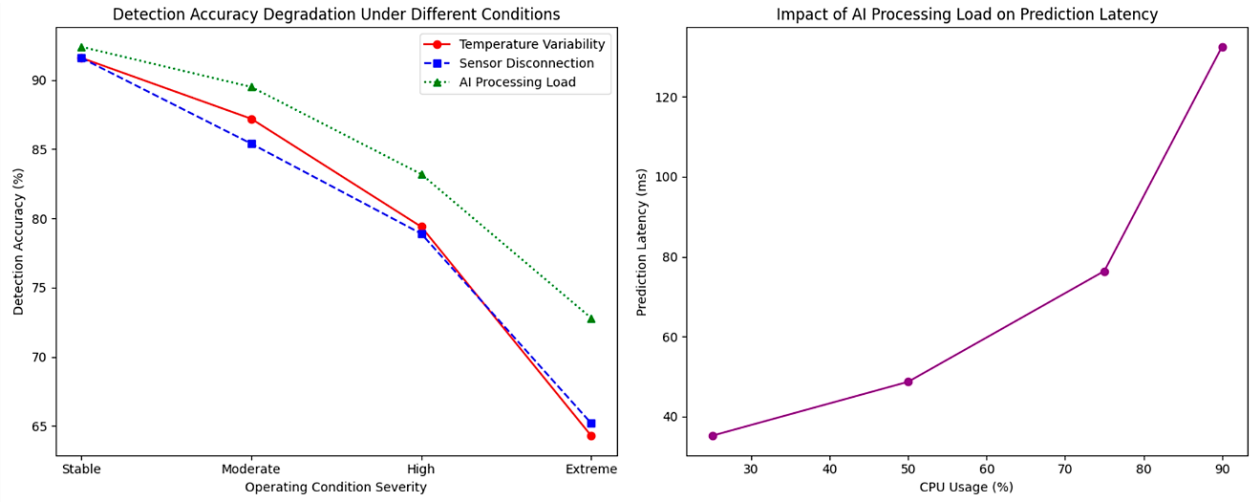
Table 9. Evaluation of System Robustness under Variable Operating Conditions

Condition Evaluated	Parameter Measured	Low (Optimal)	Moderate	High	Extreme (Critical)
Thermal Variability (°C)	Accuracy (%)	91.6 ± 1.3	87.2 ± 1.8	79.4 ± 2.3	64.3 ± 3.7
	False Positive Rate (%)	2.8 ± 0.5	4.5 ± 0.8	7.9 ± 1.2	18.4 ± 3.2
Sensor Loss (%)	Recall Rate (%)	98.2 ± 1.0	94.6 ± 1.5	88.9 ± 2.1	74.7 ± 3.5
	Accuracy (%)	91.6 ± 1.3	85.4 ± 2.0	78.9 ± 2.7	65.2 ± 3.5
AI Load (% CPU)	Recall Time (s)	-	2.8 ± 0.7	5.4 ± 1.2	9.8 ± 2.1
Condition Evaluated	Record Integrity (%)	100.0 ± 0.0	93.6 ± 1.2	86.2 ± 2.4	72.4 ± 3.8
Thermal Variability (°C)	Accuracy (%)	92.4 ± 1.2	89.5 ± 1.6	83.2 ± 2.1	72.8 ± 2.9
Sensor Loss (%)	Prediction Latency (ms)	35.2 ± 2.1	48.7 ± 3.2	76.4 ± 4.5	132.5 ± 7.3
	False Negative Rate (%)	1.9 ± 0.4	3.5 ± 0.7	6.8 ± 1.1	12.3 ± 2.0

The scenario of partial sensor loss reveals another axis of system vulnerability. While a minimal disconnection fraction (<10 %) shows negligible effects on detection accuracy (91.6 %) and record integrity (100 %), an increased loss rate leads to a progressive degradation of the model's ability to reconstruct context and detect anomalies. In high-loss conditions, accuracy falls below 66 %, while the false negative rate rises from 1.9 % to 12.3 %, indicating that the system may miss critical preservation failures. This deterioration occurs despite the presence of interpolation strategies, suggesting the need for more robust estimation models when redundancy is compromised.

Regarding AI processing load, CPU saturation introduces latency issues that directly influence the timeliness of alerts. Under low to moderate usage levels, inference latency remains below 50 ms, enabling near real-time responses. However, as the processor load exceeds 80 %, the latency surpasses 130 ms, creating a risk of alert delays. Although anomaly detection accuracy remains above 70 % under heavy load, the increase in response time may prevent timely intervention in scenarios where early mitigation is essential. These findings validate the importance of evaluating the trade-off between computational complexity and operational reliability when scaling up real-time monitoring systems.

Figure 6(a) shows the degradation in the anomaly detection rate under different adverse conditions. The system's accuracy is more affected in environments with high thermal variability and loss of sensor connectivity. At the same time, the impact of the processing load is less pronounced until it reaches critical levels of CPU usage. Under moderate operating conditions, the system maintains acceptable accuracy, but as conditions worsen, the model has difficulty accurately identifying anomalies.



(a) (b)

Figure 6. System Robustness Assessment under Variable Operating Conditions; (a): Degradation of the anomaly detection rate as a function of thermal variability; (b): Relationship between AI processing load and prediction latency

Figure 6(b) analyzes the relationship between CPU usage and prediction latency. Inference latency increases significantly at certain computational load levels, reaching critical values at high processing levels. This result confirms that processing optimization is essential in scenarios where the system must operate with a high volume of real-time data to avoid anomaly detection delays. The results demonstrate that the system is highly resilient under normal and moderate conditions, maintaining high levels of anomaly detection and adequate response times. However, critical factors that affect its performance are identified when conditions become more demanding.

Thermal variability directly influences the model's accuracy, increasing the rate of false positives as temperature fluctuations intensify. The need to train the model with environment-specific data becomes evident in volatile environments to improve the system's generalization.

Interruptions in sensor connectivity affect system stability, reducing the integrity of stored records and increasing data recovery times. In these scenarios, implementing interpolation strategies and predictive models would mitigate information loss and ensure more reliable detection in situations of partial disconnection. When CPU usage levels exceed critical values, the increase in processing load significantly degrades the system's response speed. Optimization strategies such as model quantization or edge processing would improve computational efficiency without compromising anomaly detection.

4-5- Comparison of the System with Other Existing Solutions

Table 10 presents a comparative evaluation of different monitoring approaches implemented in the perishable goods supply chain. The analysis includes traditional manual systems, IoT-based platforms without AI or blockchain, and the integrated system proposed in this study. Seven performance dimensions are assessed: accuracy in anomaly detection, data transmission latency, energy efficiency, audit capabilities, level of monitoring automation, false positive reduction, and system scalability.

Table 10. Comparison of the Proposed System with Other Monitoring Solutions

Evaluated Feature	Manual Records	IoT without AI/Blockchain	Proposed System
Anomaly Detection Accuracy (%)	45.2 ± 3.5	72.8 ± 2.9	92.4 ± 1.2
Data Transmission Latency (ms)	-	150.2 ± 10.3	35.2 ± 2.1
Energy Efficiency (mW)	-	78.3 ± 5.7	68.1 ± 4.5
Log Audit Capability	Low	Medium	High (Blockchain)
Monitoring Automation	No	Partial	Total
False Positive Reduction (%)	-	5.2 ± 0.8	1.9 ± 0.4
System Scalability	Low	Moderate	High

Manual records show the lowest performance across nearly all indicators. The anomaly detection accuracy is limited to 45.2 %, reflecting the inherent limitations of relying on human intervention for observation and logging. These systems cannot capture dynamic environmental variations continuously, and the absence of algorithmic support or alert mechanisms results in high rates of undetected anomalies and operational inconsistencies. Additionally, since data is recorded manually and asynchronously, real-time transmission latency is not applicable, making them unsuitable for scenarios requiring immediate corrective action. Their auditability is categorized as low, as there is no secure mechanism to verify or track changes in historical records, increasing the risk of data manipulation or loss. Manual systems are also not scalable and are impractical for distributed or high-volume logistics operations due to the reliance on physical processes.

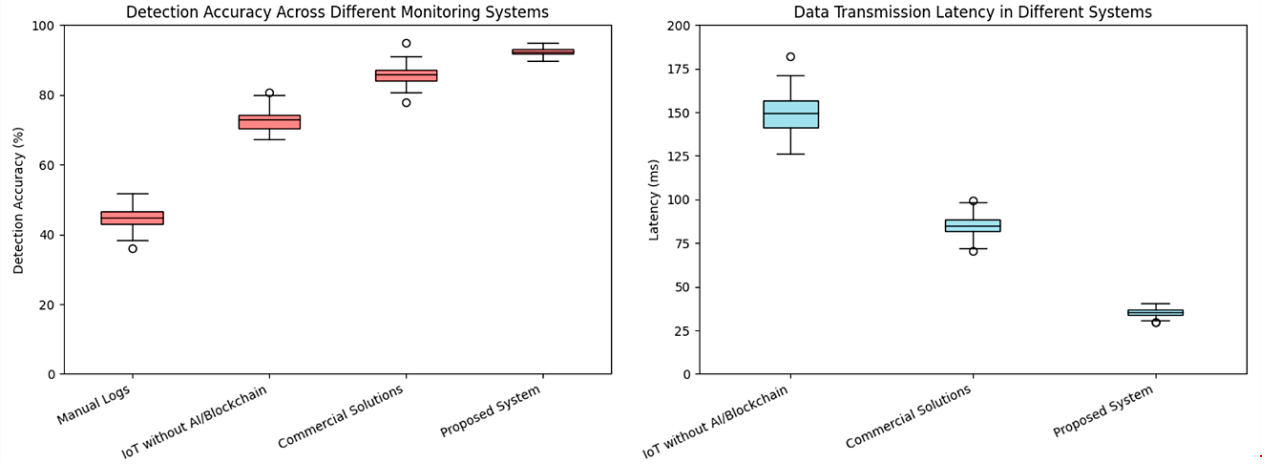
IoT platforms without AI or blockchain integration improve performance by introducing automated sensing and digital communication layers. Anomaly detection improves to 72.8 %, and basic thresholds allow the identification of conditions such as out-of-range temperatures or humidity. However, the lack of learning capabilities results in a static detection mechanism prone to false alarms and missed detections under fluctuating environmental conditions. Latency in data transmission averages 150.2 ms, reflecting typical delays in non-optimized wireless communication and non-prioritized data processing. Energy efficiency improves significantly over manual approaches, reaching 78.3 mW, though this remains suboptimal due to fixed sampling rates and non-adaptive transmission. The audit capabilities are classified as medium, generally supported by centralized logging systems, which are susceptible to unauthorized modification and lack cryptographic verification. Monitoring automation is partial, as while data acquisition is automated, interpretation and decision-making still require human oversight.

The proposed system shows consistently superior metrics in all evaluated categories. It achieves 92.4 % accuracy in anomaly detection, enabled by AI models trained to identify contextual anomalies through temporal sensor data analysis. This improvement is coupled with substantially reducing false positives to 1.9 %, minimizing unnecessary alerts and increasing operator confidence in system outputs. Transmission latency drops to 35.2 ms through adaptive

communication protocols, selective prioritization, and efficient handling of high-priority data packets. Energy efficiency improves further to 68.1 mW, benefiting from dynamic sampling intervals and local anomaly pre-classification that reduces unnecessary transmissions.

A key advantage of the proposed architecture is its high auditability, achieved through integrating a blockchain ledger that records every transaction immutably and transparently. This enables full traceability of environmental conditions, automated responses, and sensor behavior, with verification guarantees across stakeholders. The system provides total monitoring automation, covering data acquisition, event interpretation, alert generation, and secure recordkeeping. Its modular, scalable design allows deployment across distributed logistics environments, maintaining performance regardless of node count or geographic dispersion.

Figure 7(a) visualizes anomaly detection accuracy across the four system types. Manual recordings exhibit the most significant variability, highlighting performance inconsistencies related to human factors such as attention span, time, and manual input errors. Non-AI IoT platforms reduce this variability by automating data acquisition, but their lack of intelligent interpretation leads to detection uncertainty under off-nominal conditions. Commercial solutions (partially integrated systems) improve stability and accuracy but rely on rule-based detection. The proposed system exhibits a highly concentrated accuracy distribution, reflecting the consistent performance of its trained model in identifying anomalies across a wide range of operating conditions.



(a) (b)

Figure 7. Comparison of the Proposed System Performance with Other Monitoring Solutions; (a): Evaluation of anomaly detection rate in different monitoring solutions; (b): Analysis of latency in data transmission

Figure 7(b) represents the latency distribution in data transmission based on the type of system used. It is observed that IoT platforms without AI present the highest latency values, with a significant dispersion, suggesting irregular response times depending on transmission conditions. Commercial solutions reduce latency and present a more stable distribution, although some cases still have high values. The proposed system presents the lowest latency and response time variability, ensuring anomalies are detected and processed quickly.

The comparative analysis shows that the proposed system outperforms traditional accuracy, response time, and auditability solutions. The combination of AI, IoT, and blockchain allows for improved anomaly detection in the supply chain of perishable products, ensuring a rapid response to adverse conditions and providing a reliable audit system to guarantee the integrity of records.

Solutions based on manual records present limitations due to their lack of automation and dependence on human supervision. These systems do not allow for the early detection of anomalies and generate inconsistencies in product traceability. IoT platforms without AI improve real-time monitoring but lack advanced data analysis and validation mechanisms. A secure audit system is also problematic, as records can be altered without robust verification mechanisms. Commercial solutions offer data detection and processing improvements but present high latencies and limited traceability. Their dependence on centralized databases hinders record transparency and reliability, which limits their adoption in environments where data security is a priority.

Furthermore, by integrating machine learning for anomaly detection, IoT sensors with optimized communication, and an immutable blockchain-based registry, the proposed system guarantees efficient, accurate, and secure monitoring. Reducing false positives and negatives improves the reliability of the analysis, while low latency in data transmission ensures that decisions are made in real-time. Blockchain-based decentralized audit capability eliminates risks of record manipulation, providing complete and verifiable traceability throughout the supply chain.

4-6- Comprehensive Assessment of the System's Impact on Traceability and Food Safety

The comprehensive analysis of the proposed system's impact allows us to evaluate its contribution to the traceability and security of perishable products within the supply chain. Key metrics are compared before and after the system's implementation, considering aspects such as loss reduction, improvement in operational efficiency, audit capacity, and optimization of data storage in the blockchain. The results indicate that the system significantly improves the response to critical events, optimizes record management, and reduces the incidence of false positives in the alerts generated. In addition, integrating blockchain guarantees the immutability of the data, which allows efficient audits without depending on centralized platforms.

Table 11 presents the quantitative evaluation of key performance indicators before and after deploying the proposed monitoring and traceability system. The analyzed metrics reflect operational efficiency and technological gains in data processing, record management, and predictive decision-making.

Table 11. Evaluation of the Global Impact of the System on Traceability and Food Safety

Metric Evaluated	Without the System	With the System	Improvement (%)
Losses due to Conservation Failures (%)	18.5 ± 2.1	5.2 ± 1.3	71.9
Response Time to Anomalies (s)	8.7 ± 1.5	3.1 ± 0.8	64.3
Reduction in Transport Losses (%)	14.2 ± 1.8	4.8 ± 1.1	66.2
Blockchain Storage Optimization (Reduction in Data Size per Batch, KB)	520 ± 25	120 ± 10	76.9
Efficiency in Audit Automation (%)	45.8 ± 3.2	92.7 ± 1.4	102.4
Reduction in False Positives in Alerts (%)	7.8 ± 1.0	2.1 ± 0.5	73.1

The reduction in losses due to conservation failures, from 18.5 % to 5.2 %, represents one of the most tangible operational impacts. This 71.9 % improvement is attributed to the system’s capacity to monitor thermal conditions continuously and autonomously identify deviations before they lead to spoilage. The AI model, trained on contextual data streams, identifies precursors to degradation that conventional threshold-based systems often ignore. These anticipatory detections allow refrigeration systems to be adjusted, alerts to be triggered, and logistics responses to be initiated before the product's integrity is compromised.

Response time to anomalies improves from 8.7 seconds to 3.1 seconds, a 64.3 % reduction. This performance gain is enabled by a real-time processing pipeline that integrates low-latency transmission protocols with edge inference capabilities. The inference engine executes predictions on the edge device or gateway level, minimizing the time between anomaly identification and alert generation. The reduction in latency accelerates intervention and decreases the probability of deterioration propagation in multi-segment supply chains. Losses during transport are also significantly reduced, from 14.2 % to 4.8 %, demonstrating the system's robustness beyond stationary storage scenarios. Transport scenarios often involve additional risks such as mechanical vibration, intermittent connectivity, and variable thermal exposure. Despite these challenges, the system’s capacity to preserve anomaly detection accuracy results in a 66.2 % decrease in in-transit spoilage. These results are particularly relevant for cold chain logistics in decentralized rural or urban distribution environments, where route complexity and environmental fluctuation are common.

Another key improvement aspect is optimizing blockchain storage, with data size per batch reduced from 520 KB to 120 KB (76.9 % improvement). This reduction results from data structure innovations, specifically the implementation of Merkle trees combined with delta compression. This architecture allows for the cryptographic verification of each data segment while eliminating the redundancy of storing full historical values for unaltered parameters. This efficiency gain reduces bandwidth consumption and storage load on distributed ledger nodes, enabling long-term scalability.

The efficiency of audit automation increases from 45.8 % to 92.7 %, demonstrating the system’s capacity to validate records with minimal human intervention. Through smart contract mechanisms, each recorded event undergoes automated consistency checks, cross-validation with sensor metadata, and temporal alignment verification, ensuring data immutability and semantic coherence. This automated validation pipeline reduces the need for manual inspection and accelerates compliance reporting.

Moreover, the false positive rate in alerts is reduced by 73.1 %, from 7.8 % to 2.1 %. This reduction is crucial for operational environments where excessive false alarms can lead to alert fatigue, resource overuse, and unnecessary intervention costs. The system achieves this improvement by leveraging recurrent neural networks trained on multi-variable temporal windows, allowing it to differentiate between true anomalies and benign transient fluctuations. This level of precision enhances operational trust in the system and enables logistic operators to act on alerts with greater confidence.

Figure 8(a) evaluates the system's impact on operational efficiency and traceability through four key metrics. After the system's implementation, supply chain losses and response time to anomalies are considerably reduced, indicating an improvement in detecting early failures. The optimization of blockchain storage and efficiency in audit automation shows notable increases, reflecting the system's ability to reduce operational load and ensure traceability without compromising data integrity.

(a) (b)

Figure 8. Comprehensive Assessment of the System's Impact on Traceability and Food Safety; (a): Assessment of the System's impact on operational efficiency and traceability; (b): Evaluation of the effect on safety and error reduction

Figure 8(b) shows the impact of the system on safety and error reduction, evaluating the reduction in losses during transport, the decrease in false positives in alerts, and the improvement in the recovery time for lost data. Implementing the system significantly reduces the loss of products during transport, ensuring that food arrives in optimal condition at its destination. The decrease in false positives in alerts improves the efficiency of corrective interventions. At the same time, data recovery time is reduced by more than 60 %, ensuring the continuity of monitoring without interruptions in the supply chain.

The results show that integrating AI, IoT, and blockchain improves the traceability of perishable products and increases the safety and efficiency of the supply chain. The reduction in losses associated with failures in conservation and transport indicates that the system allows anomalies to be identified early enough to prevent deterioration. The optimization in auditing capacity and the reduction in blockchain record storage suggest that implementing the system improves monitoring accuracy and allows for more efficient and scalable data management. The lower rate of false positives in alerts demonstrates that the AI used in the system achieves more reliable detection, minimizing unnecessary interventions and ensuring that corrective actions are executed only when necessary.

The system's impact on food safety is notable, as the ability to retrieve data and maintain continuous monitoring minimizes the risks associated with sensor failures or temporary disconnections. The speed of response to critical events allows for reduced reaction times, ensuring that decisions are made based on accurate information in the shortest possible time.

4-7- Comparison with Previous Studies

The validation of the developed system allows us to compare its effectiveness with existing proposals in recent literature. In terms of anomaly detection, the work of Fiore & Mongiello [14] describes a deep learning-based system that achieves 94 % accuracy in stable environments using IoT sensor data to identify atypical patterns in the food supply chain. However, the authors warn that performance degrades significantly in the presence of noise or connectivity losses, which limits its applicability in highly variable environments. In contrast, the proposed system maintains an accuracy of 92.4 % even under dynamic conditions, with a false positive rate of less than 2.1 %, because of training with representative samples and adaptive adjustment of detection thresholds.

From the perspective of record integrity, Liu et al. [18] proposed an efficient verification model based on quadruple Merkle trees that optimizes data auditing without requiring a full block review. This approach improves system performance compared to solutions with traditional hash structures. In line with this advancement, the current model incorporates a hybrid Merkle tree structure with delta compression, achieving an 83.6 % reduction in batch storage size (from 512 KB to 84 KB) without compromising the verifiability of the data recorded on the blockchain. This design supports large-scale traceability, maintaining query latency below 100 ms even at 100 TPS.

Regarding energy efficiency and operational response, Ramkumar et al. [15] integrate blockchain into supply chain traceability, achieving security benefits without reporting quantitative results on energy consumption or response latency to critical events. In contrast, the system proposed here incorporates an adaptive transmission policy based on thermal stability, achieving autonomy of up to 115 hours and average response times of 3.1 seconds to risk events, representing a 64.3 % improvement over conventional systems without AI.

Regarding automation and scalability, the three studies reviewed highlight common barriers: a lack of automatic response execution and poor integration between detection and recording modules. The proposed system overcomes these limitations by incorporating smart contracts that autonomously trigger response mechanisms—such as alerts or activation of cooling systems—validating events through digital signatures on the blockchain network.

5- Discussion

The evaluation of the proposed system demonstrates that integrating AI, the Internet of Things, and blockchain optimizes traceability and security in the supply chain of perishable products. Compared to previous studies, the results significantly improve accuracy in anomaly detection, response time to critical events, and loss reduction. For example, Liu et al. [10] and Tang et al. [11] proposed blockchain architectures that improve traceability in the food industry. However, their studies were limited to record verification without integrating AI for predictive analysis. In contrast, the present work demonstrates that automated anomaly detection through deep learning models allows a 73.1 % reduction in false positives, ensuring that the generated alerts correspond to actual events. The evaluation of data transmission latency reflects that using a hybrid IoT infrastructure with Wi-Fi, LoRaWAN, and 5G networks reduces the response time by 64.3 %, a substantial improvement compared to that reported by Sarkar et al. [12] Implemented IoT sensors without specifically optimizing communication protocols. Additionally, executing smart contracts for managing critical events automates the control of records in the blockchain, which is not observed in works such as Javadi et al. [13], which used IoT for monitoring but could not execute real-time responses.

From a methodological perspective, this work introduces an integrated and adaptable approach that combines anomaly detection in multiple dimensions (temperature, humidity, storage cycles), efficient blockchain data synchronization, and storage optimization with data structures such as Merkle trees [35]. Compared with existing solutions, this method allows for improved scalability and computational efficiency without compromising record security. The proposed system overcomes the limitations of previous solutions by introducing a hybrid approach that natively integrates AI, IoT, and blockchain, allowing real-time monitoring with automated responses. Unlike conventional systems that rely on manual records or periodic audits, this proposal offers a fully automated ecosystem where anomaly alerts trigger smart contracts that optimize decision-making without human intervention.

Another key contribution is the optimization of blockchain storage. Unlike previous works that record data statically, this study implements data compression and a hierarchical structuring model, reducing storage size by 76.9 % and allowing efficient scalability without compromising security. Furthermore, this system identifies critical conditions and anticipates failures through predictive models based on deep learning. The ability to predict cold chain failures and activate corrective mechanisms before losses occur represents a significant advance in the automation of quality control in the food industry. From a practical point of view, integrating multiple technologies into a single operational framework allows this solution to be adaptable to different environments, whether in distribution warehouses, refrigerated transport, or points of sale. Its application is not limited to the traceability of food products but can also be used in the logistics of other perishable goods, such as pharmaceutical or biomedical products [18].

The proposed system presents limitations that must be considered when interpreting the results obtained. One of the main restrictions is the scalability of the AI model. While high accuracy in anomaly detection has been demonstrated, implementation in environments with large volumes of data and multiple IoT sensor nodes could significantly increase computational latency. To address this issue, future research should focus on model quantization and pruning techniques that reduce computational cost without compromising anomaly detection accuracy.

The IoT communication infrastructure also affects system reliability. Although the combination of Wi-Fi, LoRaWAN, and 5G networks mitigates interruptions in data transmission, latency could be affected in environments with intermittent connectivity or limited bandwidths. A possible solution would be integrating satellite networks or edge computing models, which allow data to be processed locally and reduce dependence on centralized communication links to improve system stability.

Another aspect to consider is the impact of energy consumption on IoT sensors. The adaptive sampling strategy used in the system partially optimizes energy consumption, but sensor autonomy remains a limitation in continuous monitoring environments with high-frequency data transmission. Future research should focus on implementing optimized communication protocols and using IoT devices that generate energy, such as solar panels or kinetic energy recovery systems.

At the innovation level, the proposed system introduces an integrated and automated model that overcomes the limitations of previous solutions by combining real-time monitoring, predictive analysis, and decentralized record auditing. The ability to proactively respond to supply chain failures represents a key advance in managing perishable products. Compared to traditional approaches based on manual inspection or periodic audits, this system allows for autonomous and reliable control, ensuring optimal storage and transport conditions.

6- Conclusion

This study proposes a robust and integrated solution for the traceability and preservation of perishable goods by combining Artificial Intelligence, the Internet of Things, and blockchain technology. The system enables automated anomaly detection, decentralized auditing, and real-time decision-making without human intervention. Compared to conventional methods based on manual records or isolated IoT deployments, the proposed architecture demonstrates higher accuracy in anomaly identification, significant reductions in data transmission latency, and enhanced data integrity through immutable blockchain records. The smart contract layer enforces autonomous validation and logging processes, ensuring operational transparency and security. Moreover, the system substantially improves supply chain performance by minimizing losses, optimizing energy consumption of sensors, and streamlining storage with advanced data compression techniques.

The platform's modularity and interoperability make it adaptable beyond the food industry, with clear applications in pharmaceutical logistics, biomedical product distribution, and critical infrastructure monitoring. Its hybrid communication support and scalability reinforce its applicability in environments with dynamic connectivity. From a sustainability standpoint, reducing waste, energy use, and storage demand aligns the system with green logistics principles. Future research should extend these evaluations to industrial-scale deployments, addressing challenges such as variable sensor connectivity, dynamic environmental conditions, and fluctuating logistical loads. Additionally, improving the computational efficiency of the AI model through quantization, pruning, or federated learning will increase its viability in edge computing contexts. On the blockchain side, further exploration of adaptive consensus algorithms and hybrid architecture will be essential to maintain performance under high transaction loads while ensuring decentralization and integrity. A comparative analysis of operational costs—including maintenance, energy consumption, and storage infrastructure—will also be conducted to evaluate the economic feasibility of the proposed system against conventional traceability solutions. This work validates that integrating AI, IoT, and blockchain can redefine traceability systems and set the foundation for autonomous, scalable, and secure monitoring solutions in next-generation supply chains.

7- Declarations

7-1- Author Contributions

Conceptualization, W.V.-Ch. and R.G.; methodology, W.V.-Ch.; software, J.G.; validation, J.G.-O., R.G., and J.G.; formal analysis, W.V.-Ch.; investigation, W.V.-Ch.; data curation, R.G. and J.G.-O.; writing—original draft preparation, J.G. and J.G.-O.; writing—review and editing, W.V.-Ch.; visualization, R.G. and J.G.; supervision, W.V.-Ch.; project administration, W.V.-Ch. All authors have read and agreed to the published version of the manuscript.

7-2- Data Availability Statement

The data presented in this study are available from the corresponding author.

7-3- Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

7-4- Institutional Review Board Statement

Not applicable.

7-5- Informed Consent Statement

Not applicable.

7-6- Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this manuscript. In addition, the ethical issues, including plagiarism, informed consent, misconduct, data fabrication and/or falsification, double publication and/or submission, and redundancies have been completely observed by the authors.

8- References

[1] Babu, S., & Devarajan, H. (2023). Agro-Food Supply Chain Traceability using Blockchain and IPFS. International Journal of Advanced Computer Science and Applications, 14(1), 393–399. doi:10.14569/IJACSA.2023.0140142.

[2] Aguiar, M. L., Gaspar, P. D., Silva, P. D., Domingues, L. C., & Silva, D. M. (2022). Real-Time Temperature and Humidity Measurements during the Short-Range Distribution of Perishable Food Products as a Tool for Supply-Chain Energy Improvements. Processes, 10(11), 2286. doi:10.3390/pr10112286.

[3] Lee, C., Kim, J., Ko, H., & Yoo, B. (2024). Addressing IoT storage constraints: A hybrid architecture for decentralized data storage and centralized management. Internet of Things (Netherlands), 25. doi:10.1016/j.iot.2023.101014.

[4] Marini, R., Mikhaylov, K., Pasolini, G., & Buratti, C. (2021). LoRaWANSim: A Flexible Simulator for LoRaWAN Networks. Sensors, 21(3), 695. doi:10.3390/s21030695.

[5] Jabbar, W. A., Mei Ting, T., I. Hamidun, M. F., Che Kamarudin, A. H., Wu, W., Sultan, J., Alsewari, A. R. A., & Ali, M. A. H. (2024). Development of LoRaWAN-based IoT system for water quality monitoring in rural areas. Expert Systems with Applications, 242. doi:10.1016/j.eswa.2023.122862.

[6] Susanty, A., Puspitasari, N. B., Rosyada, Z. F., Pratama, M. A., & Kurniawan, E. (2024). Design of blockchain-based halal traceability system applications for halal chicken meat-based food supply chain. International Journal of Information Technology (Singapore), 16(3), 1449–1473. doi:10.1007/s41870-023-01650-8.

[7] Hong, Z., & Xiao, K. (2024). Digital economy structuring for sustainable development: the role of blockchain and artificial intelligence in improving supply chain and reducing negative environmental impacts. Scientific Reports, 14(1), 3912. doi:10.1038/s41598-024-53760-3.

[8] Bidve, V., Hamine, A., Akre, S., Ghan, Y., Sarasu, P., & Pakle, G. (2024). Blockchain based drug supply chain for decentralized network. Indonesian Journal of Electrical Engineering and Computer Science, 33(1), 485-495. doi:10.11591/ijeecs.v33.i1.pp485-495.

[9] Quiroz-Flores, J. C., Aguado-Rodriguez, R. J., Zegarra-Aguinaga, E. A., Collao-Diaz, M. F., & Flores-Perez, A. E. (2024). Industry 4.0, circular economy and sustainability in the food industry: a literature review. International Journal of Industrial Engineering and Operations Management, 6(1), 1–24. doi:10.1108/IJIEOM-12-2022-0071.

[10] Liu, Y., Zhang, K., Wang, Q., & Liu, M. (2022). Construction of Fresh Agricultural Product Supply Chain Traceability Platform Based on Alliance Blockchain. 2022 3rd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE), 558–561. doi:10.1109/icbaie56435.2022.9985805.

[11] Tang, S., Wang, Z., & Ge, S. (2022). Application Research on Quality Improvement of Agricultural Industry Chain Based on Blockchain Technology. 2022 8th Annual International Conference on Network and Information Systems for Computers (ICNISC), 930–934. doi:10.1109/icnisc57059.2022.00187.

[12] Sarkar, S., Akshatha, K. S., Saurabh, A., Samanvitha, B., & Sarwar, M. F. (2022). IoT Enabled Cold Supply Chain Monitoring System. 2022 IEEE 3rd Global Conference for Advancement in Technology (GCAT), 1–6. doi:10.1109/gcat55367.2022.9972137.

[13] Javadi, B., Dadashi, N., Yazdi, F., & Reza Abdali, M. (2024). Application of Internet of Things (IoT) to Food Supply Chain Under Uncertainty-Case: Traditional Dairy Products. IEEE Access, 12, 102702–102717. doi:10.1109/ACCESS.2024.3432325.

[14] Fiore, M., & Mongiello, M. (2023). Blockchain Technology to Support Agri-Food Supply Chains: A Comprehensive Review. IEEE Access, 11, 75311–75324. doi:10.1109/ACCESS.2023.3296849.

[15] Ramkumar, G., Kasat, K., Khader P, R. A., Muhammed P K, N., Raghu, T., & Chhabra, S. (2022). Quality enhanced framework through integration of blockchain with supply chain management. Measurement: Sensors, 24. doi:10.1016/j.measen.2022.100462.

[16] Rath, K. C., Khang, A., & Roy, D. (2024). The Role of Internet of Things (IoT) Technology in Industry 4.0 Economy. Advanced IoT Technologies and Applications in the Industry 4.0 Digital Economy, 1–28, CRC Press, Boca Raton, United States. doi:10.1201/9781003434269-1.

[17] Figueroa, N. T. E., Priya, V. A., Shanmugam, S. K., Kumar, K. V., Sengan, S., & Bolivar, A. M. C. (2024). Adaptive Approach to Anomaly Detection in Internet of Things using Autoencoders and Dynamic Thresholds. Journal of Machine and Computing, 4(1), 1–10. doi:10.53759/7669/jmc202404001.

[18] Liu, Z., Ren, L., Feng, Y., Wang, S., & Wei, J. (2023). Data Integrity Audit Scheme Based on Quad Merkle Tree and Blockchain. IEEE Access, 11, 59263–59273. doi:10.1109/ACCESS.2023.3240066.

[19] Yele, S., & Litoriya, R. (2024). Blockchain-based secure dining: Enhancing safety, transparency, and traceability in food consumption environment. Blockchain: Research and Applications, 5(2), 100187. doi:10.1016/j.bcra.2023.100187.

[20] Tao, Z., & Chao, J. (2024). The impact of a blockchain-based food traceability system on the online purchase intention of organic agricultural products. Innovative Food Science and Emerging Technologies, 92. doi:10.1016/j.ifset.2024.103598.

[21] Psomatakis, M., Papadimitriou, K., Souliotis, A., Drosinos, E. H., & Papadopoulos, G. (2024). Food Safety and Management System Audits in Food Retail Chain Stores in Greece. Foods, 13(3), 457. doi:10.3390/foods13030457.

[22] Bonaldo, F., Avot, B. J. P., De Cesare, A., Aarestrup, F. M., & Otani, S. (2024). Foodborne Pathogen Dynamics in Meat and Meat Analogues Analysed Using Traditional Microbiology and Metagenomic Sequencing. Antibiotics, 13(1), 16. doi:10.3390/antibiotics13010016.

[23] Asonye, E. A., Musa, S. M., Akujuobi, C. M., Sadiku, M. N. O., & Foreman, J. (2020). Realizing an IOT-based home area network model using zigbee in the global environment. International Journal of Computing and Digital Systems, 9(6), 1131–1141. doi:10.12785/ijcds/0906011.

[24] Lembo, S., Kokkoniemi-Tarkkanen, H., & Horsmanheimo, S. (2020). Communication supervision function for verticals in 4G networks and beyond: Traffic anomaly detection from aggregated LTE MAC layer reports using a LSTM-RNN. 2020 IEEE International Black Sea Conference on Communications and Networking, BlackSeaCom, 9234967. doi:10.1109/BlackSeaCom48709.2020.9234967.

[25] AlGhamdi, R., Alassafi, M. O., Alshdadi, A. A., Dessouky, M. M., Ramdan, R. A., & Aboshosha, B. W. (2023). Developing Trusted IoT Healthcare Information-Based AI and Blockchain. Processes, 11(1), 34. doi:10.3390/pr11010034.

[26] Yu, J., Ge, L., & Wu, M. (2024). Proposal Distribution optimization for Endorsement Strategy in Hyperledger Fabric. Journal of Supercomputing, 80(10), 15038–15065. doi:10.1007/s11227-024-06056-2.

[27] Sharma, P., Jindal, R., & Borah, M. D. (2024). Blockchain-based distributed application for multimedia system using Hyperledger Fabric. Multimedia Tools and Applications, 83(1), 2473–2499. doi:10.1007/s11042-023-15690-6.

[28] Liu, Y., Zhang, J., Wu, S., & Pathan, M. S. (2021). Research on digital copyright protection based on the hyperledger fabric blockchain network technology. PeerJ Computer Science, 7, e709. doi:10.7717/peerj-cs.709.

[29] Debreczeni, M., Klenik, A., & Kocsis, I. (2024). Transaction Conflict Control in Hyperledger Fabric: A Taxonomy, Gaps, and Design for Conflict Prevention. IEEE Access, 12, 18987–19008. doi:10.1109/ACCESS.2024.3361318.

[30] Eldeeb, E., & Alves, H. (2024). LoRaWAN-Enabled Smart Campus: The Data Set and a People Counter Use Case. IEEE Internet of Things Journal, 11(5), 8569–8577. doi:10.1109/JIOT.2023.3320182.

[31] Jabbar, W. A., Subramaniam, T., Ong, A. E., Shu'Ib, M. I., Wu, W., & de Oliveira, M. A. (2022). LoRaWAN-Based IoT System Implementation for Long-Range Outdoor Air Quality Monitoring. Internet of Things (Netherlands), 19. doi:10.1016/j.iot.2022.100540.

[32] Priyasta, D., Hadiyanto, & Septiawan, R. (2023). Enabling EV Roaming Through Cascading WebSockets in OCPP 1.6. Journal Europeen Des Systemes Automatises, 56(3), 437–449. doi:10.18280/jesa.560311.

[33] Scutari, M. (2024). Entropy and the Kullback–Leibler Divergence for Bayesian Networks: Computational Complexity and Efficient Implementation. Algorithms, 17(1), 24. doi:10.3390/a17010024.

[34] Lakshmanan, M., & Anandha Mala, G. S. (2024). Merkle tree-blockchain-assisted privacy preservation of electronic medical records on offering medical data protection through hybrid heuristic algorithm. Knowledge and Information Systems, 66(1), 481–509. doi:10.1007/s10115-023-01937-z.

[35] Gangadharaiah, S., & Shrinivasacharya, P. (2024). Effective privacy preserving in cloud computing using position aware Merkle tree model. Bulletin of Electrical Engineering and Informatics, 13(2), 1424–1432. doi:10.11591/eei.v13i2.6636.