Uluslararası İleri Doğa Bilimleri ve Mühendislik Araştırmaları Dergisi
Sayı 10, S. 259-269, 3, 2026
© Telif hakkı IJANSER'e aittir
Araştırma Makalesi

https://as-proceeding.com/index.php/ijanser
ISSN: 2980-0811

International Journal of Advanced Natural Sciences and Engineering Researches
Volume 10, pp. 259-269, 3, 2026
Copyright © 2026 IJANSER
ResearchArticle

Secure Cold Chain Product Tracking Using IoT and Blockchain Network

Talha Dağ[1], Gamze Varol[2], Yunus Santur[3]

[1,2,3] Department of Artificial Intelligence and Data Engineering, Faculty of Engineering-Faculty, Fırat University, Elazığ, Türkiye

[1] talha.dag2005@gmail.com, [2] gmzvrl04@gmail.com, [3] ysantur@firat.edu.tr

(Received: 26 March 2026, Accepted: 30 March 2026)

(7th International Conference on Contemporary Academic Research ICCAR 2026, March 25-26, 2026)

ATIF/REFERENCE: Dağ, T., Varol, G. & Santur, Y. (2026). Secure Cold Chain Product Tracking Using IoT and Blockchain Network, *International Journal of Advanced Natural Sciences and Engineering Researches*, 10(3), 259-269.

Abstract – This research introduces a hybrid tracking system that utilizes Internet of Things (IoT) and blockchain technology to secure and facilitate transparent logistics of critical goods like pharmaceuticals and perishable food items. The safety of products is compromised by traditional cold chain management., which involves central server failures and data manipulation. The proposed model uses DHT11 temperature and humidity sensors and GPS sensors to collect data that is processed with the assistance of an ESP32 microcontroller with the data being tracked on the Ethereum test network through smart contracts. In the case where the value of temperature exceeds the defined maximum (which is 4 degrees Celsius), the system will automatically generate a record of violation with the respective data being stored in the ledger of the blockchain on an irreversible basis. The results of the experiments demonstrated that the system could provide real-time monitoring and protection of data. This technical solution has the potential to reduce food wastage and provide full transparency in the logistics process.

Keywords – IoT, blockchain, cold chain, traceability, food safety.

I. INTRODUCTION

The cold chain is a temperature-controlled supply chain system aimed at preserving product quality and ensuring safety during the process from production to shipment, storage, and consumption of perishable products such as food, pharmaceuticals, and chemicals. Driven by technological transformation, global cold chain operations are projected to grow from a volume of $365.78 billion in 2024 to an economic size exceeding $1.4 trillion by 2034, with a compound annual growth rate (CAGR) of 14.5% [1]. Administrative and technical failures within this system directly and adversely affect the shelf life and safety of products. Even a deviation of a few degrees beyond the specified temperature limits causes the rapid proliferation of microorganisms and food spoilage, thereby threatening public health. Today, approximately 1.05 billion tons of food are wasted globally every year; this amount constitutes about one-fifth of the total food available for consumption worldwide, leading to massive environmental and economic losses [2], [3]. The inadequacy of traditional monitoring systems in terms of transparency, real-time data provision, and data security has made the integration of technology-oriented smart solution mechanisms into the system imperative, especially for tracking perishable goods [4], [5].

The Internet of Things (IoT) architecture is a technology that enables physical objects to communicate seamlessly with each other over the internet and operate synchronously, utilizing smart sensors, gateways, and cloud-based data processing units [6]. A standard IoT system is a dynamic structure consisting of smart devices that collect data from the environment, applications that analyze this data, and a graphical user interface that manages the system [7]. In the context of cold chain logistics, IoT sensors enable the simultaneous tracking of environmental parameters such as temperature, humidity, and vibration in the environments where products are located, ensuring that every moment of the process is traceable. By replacing manual data entry with an automated recording system, this autonomous infrastructure provides a reliable framework that minimizes human error, thereby eliminating the risks posed by manual data recording methods [8]. Thanks to sensor analytics, instant intervention mechanisms are triggered when the specified threshold value is deviated, preventing product losses before they occur.

However, one of the major problems encountered in IoT systems is the rapid proliferation of generated devices and data [9]. Storing the data obtained from IoT devices in traditional centralized server systems renders the system a vulnerable target against cybersecurity threats. These devices, which communicate over a centralized network, carry the risk of a single point of failure (SPOF) and harbor the possibility of data manipulation [5], [9]. This situation leads to a lack of transparency and trust issues among stakeholders in the supply chain.

To overcome these vulnerabilities regarding data verifiability, immutability, and integrity, the integration of blockchain technology into IoT systems has become a critical necessity. Using asymmetric encryption methods and consensus algorithms, blockchain guarantees that all executed transactions are recorded in a decentralized, transparent, and retrospectively immutable digital ledger. Its independence from a central authority technically prevents unauthorized external interference attempts and maximizes data security [5], [10]. Through the integration of IoT and blockchain technologies, real-time data obtained from field sensors becomes instantaneously traceable by all stakeholders in a transparent manner [11]. This integrated structure detects temperature deviations instantly, enabling the generation of autonomous alerts, reducing the risk of counterfeiting, and elevating efficiency in logistics processes to the highest level.

A review of the academic literature reveals various studies examining the transformative effects of IoT and blockchain-based technologies on supply chain management. Ben-Daya et al. (2019) investigated the theoretical impacts of IoT on supply chain management, but the analytical depth of the sensors utilized was left out of the evaluation scope [12]. In recent research, Rejeb et al. (2020) conducted a bibliometric analysis of IoT research in supply chain and logistics, but did not delve into the hardware and application details required for IoT-based systems [13]. Similarly, while analyzing the impact of IoT on supply chain management processes, Rebelo et al. (2022) excluded the application areas of field sensors from their research [14]. Hussain et al. (2021) conducted a systematic literature review of blockchain-based IoT devices; however, they highlighted the lack of comprehensive analytical application models in the literature where physical sensor data is directly integrated with autonomous smart contracts [9].

The model developed within the scope of this research aims to fill this hardware and analytical gap identified in the literature. The proposed hybrid model combines IoT and blockchain technology to ensure the transparent logistics of products directly related to public health, such as pharmaceuticals and perishable foodstuffs. Considering industrial applicability and cost-effectiveness, the low-cost and highly energy-efficient ESP32 microcontroller is positioned as the main management center in this study. Environmental data collected by the DHT11 temperature/humidity sensors and GPS modules integrated into the system is processed through this microcontroller and instantly monitored via smart contracts on the Ethereum test network. When the defined temperature thresholds (e.g., 4°C) are exceeded, the system automatically creates a violation record, and this data is recorded on the blockchain ledger in an irreversibly immutable manner. This model, representing a highly commercial and field-applicable solution, aims to prevent food waste by providing full transparency in logistics processes and to build a more sustainable future in line with the "Green Deal" objectives.

II. MATERIALS AND METHOD

In this study, a hybrid system model integrating Internet of Things (IoT) and Blockchain technologies has been developed to ensure the safety and enhance the traceability of highly temperature-sensitive products, such as food, pharmaceuticals, and chemicals, during supply chain processes. Cold chain logistics is of critical importance for the preservation of product quality [3], [15]. The aim is to overcome problems encountered in traditional methods, such as data manipulation, lack of transparency, and centralized server failures [9]. The proposed system is based on the principle of collecting environmental data (temperature, humidity) in real-time via sensors, transmitting this data over a secure network by encrypting it, and storing it immutably within a decentralized ledger technology (DLT) structure [5], [16]. In this section, the layered architecture of the system, hardware components, and the algorithms governing the decision-making mechanism are detailed.

A. *System Architecture*

The cold chain monitoring system developed in this research features a layered architecture to ensure end-to-end data transmission and information security. As shown in Figure 1, the theoretical infrastructure of the designed system architecture consists of three layers—Sensing, Network, and Application—to define the basic data flow and the practical implementation of the application.

The architecture consists of the following fundamental elements, and the data communication between the layers is as follows:

Sensing layer (Blue area): The lowest layer of the framework includes the edge units that collect information about the physical environment. The DHT11 (temperature/humidity sensing), PIR (motion sensing), and GPS modules used in this research project send analog and digital environmental data to the main controller [7], [17]. The acquired data is processed and converted into digital format using an ESP32/Arduino microcontroller.

Network layer (Green area): The data received from the sensors is uploaded to the internet via the IoT Gateway (Data Collection Point), thereby reaching the network layer. At this level, to ensure data consistency during device communication, the information is packaged in JSON format, encrypted, and directed to the application layer using secure communication protocols (HTTPS/MQTT) [18].

Application layer (Orange area): This is the third layer that manages the decision-making process of the system. Pre-determined temperature limits (T > 4°C) are evaluated by Smart Contracts on the Ethereum Test Network. When the temperature exceeds the pre-determined threshold, the system automatically generates an alert and immutably records this as a permanent entry on the blockchain [5], [16]. End-users can monitor the product status and blockchain records in real-time through a mobile or web-based monitoring dashboard.

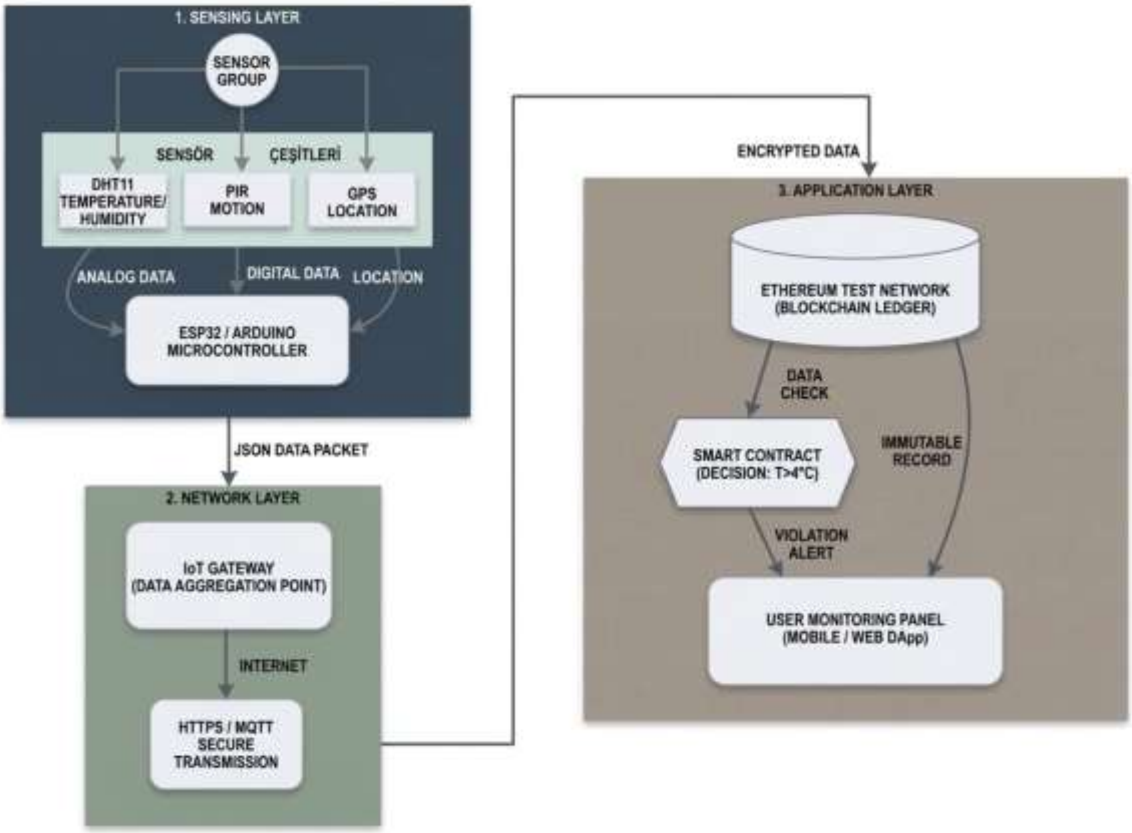


Figure 1. Detailed system architecture of the proposed IoT and blockchain integration.

B. *Hardware components*

In the prototype stage of the system, industrial applicability and cost-effectiveness criteria were taken into consideration. The ESP32 Azure IoT Kit and Arduino-based boards were selected as the main controllers. Thanks to its built-in Wi-Fi/Bluetooth modules and low power consumption, the ESP32 is capable of processing sensor data in real-time [18], [19].

DHT11 temperature and humidity sensors were integrated into the system to monitor environmental conditions. These sensors are capable of measuring within the range of 0°C to 50°C to detect critical changes in the cold chain [4], [8]. Furthermore, motion sensors were included in the system to ensure the physical security of the products and to detect unauthorized interventions. Data read from the sensors is structured in JSON format and transmitted to the network. The data collected from the sensors is structured in JSON format in order to optimize network traffic. The structure and sample values of the generated data packet are presented in Table 1.

Table 1. Structure and parameters of the data packet sent from the IoT device.

Parameter	Data Type	Sample Value	Description
device_id	String	"SENSOR_001"	Unique identification number of the device.
timestamp	DateTime	"2025-12-15 14:30"	Date and time when the data was read.
temperature	Float	4.2	Temperature read from the DHT11 sensor (°C).
humidity	Float	65.5	Relative humidity rate in the environment (%).
location	Object	{"lat": 38.35, "lon": 38.30}	Latitude/longitude obtained from the GPS module.

C. *Software and smart contract algorithm*

Data security is the most critical factor in cold chain logistics [5]. In this study, Decentralized Blockchain Technology was utilized to ensure data immutability [9], [16]. Data received from IoT devices is transmitted directly to smart contracts.

Smart contracts are autonomous scripts that execute automatically when predefined conditions (e.g., "Temperature > 4°C") are met. The decision-making mechanism of the system is modeled by Equation 1, utilizing the temperature *T(t)* at time t and the threshold value T_{max}.

$$f(t) = \begin{cases} 1(\text{Violation}), & T(t) > T_{max} \\ 0(\text{Normal}), & T(t) \leq T_{max} \end{cases}$$

Equation 1. The decision-making mechanism model of the system based on the temperature *T(t)* at time t and the threshold value T_{max}.

Here, the condition f(t) = 1 represents the state in which the smart contract is triggered, and a "Violation" record is logged into the blockchain ledger. Through this method, the retroactive manipulation of data is rendered impossible [20]. The operation of the violation detection algorithm is presented in Algorithm 1.

Algorithm 1. Cold Chain Violation Detection and Blockchain Recording Logic

```
Input: Sensor_Temperature, Threshold_Value (4°C)
Output: Blockchain_Transaction

Start
$T_{\text{current}}$: Read Temperature Data from Sensor
IF $T_{\text{current}}$ > Threshold_Value) THEN
    Status: "Critical_Violation"
    Trigger_Alarm()
    Blockchain_Write (Status, Time, Hash)
ELSE
    Status: "Normal"
    Blockchain_Write (Status, Time, Hash)
END IF
End
```

III. RESULTS

A. *Test Scenario and Simulation Infrastructure*

Before proceeding to the hardware phase, the software and blockchain performance of the developed system were tested on a large-scale hybrid dataset (10,995 transaction records) created by blending and synthetically enriching (data augmentation) two different open-source datasets representing real-world logistics processes for simulation purposes [21], [22]. In the test scenario, the real-time data anticipated from the IoT devices was simulated in a computer environment; by deliberately raising the temperature values above the 4°C critical threshold, the response time and recording accuracy of the Smart Contracts were measured using the facilities of Fırat University. In the physical implementation phase of the project, it is aimed to directly integrate real-time environmental data into the system by utilizing ESP32 and DHT11 sensors instead of these simulated data.

B. *Temperature Tracking and Violation Analysis*

The dynamic analysis outputs, generated from the data acquired from the system, reported every temperature variation affecting product quality throughout the logistics process. Out of more than 10,000 processed transactions, products that exceeded the temperature threshold or whose quality was found to be degraded were autonomously classified into the "Risk" category by the system without any human intervention (See Figure 2).

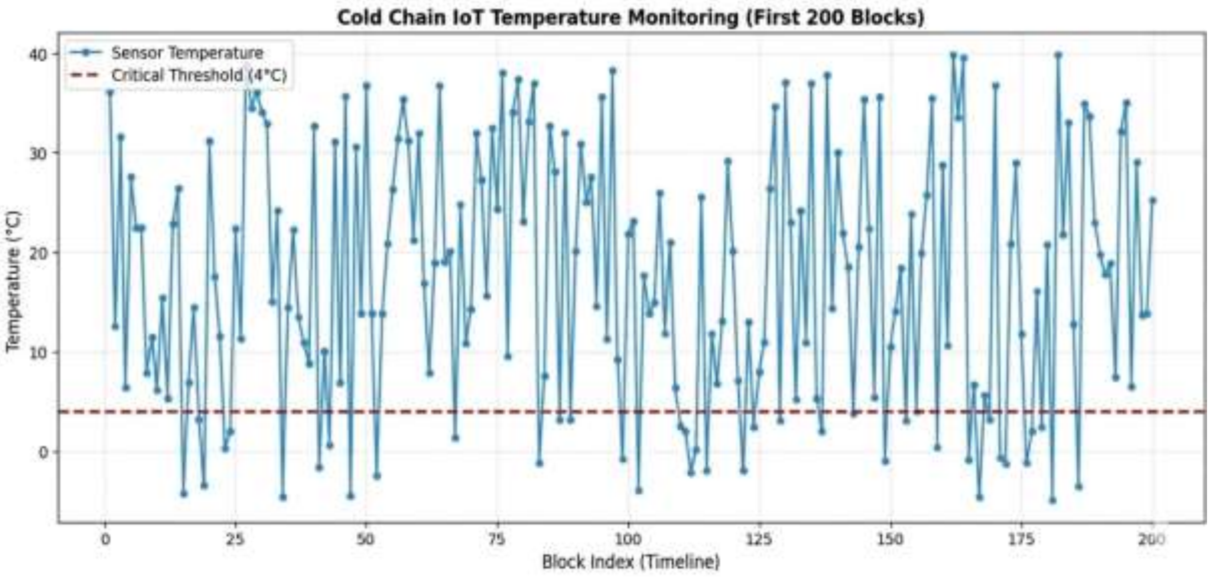


Figure 2. Temperature variation and 4°C critical threshold violation graph based on IoT sensor data.

C. Blockchain Ledger Outputs

As the core component of our system, the encrypted blockchain ledger showed flawless performance during data integrity testing. We applied the SHA-256 cryptographic algorithm to lock every piece of incoming shipment data. After encryption, the system assigns a unique digital hash and securely adds the record to the chain (See Figure 3). Our evaluation confirmed a strict end-to-end connection: every single block actively references the exact hash of the one immediately before it (Previous_Hash). This continuous linkage clearly proves that no data corruption or tampering occurred.

Furthermore, not only the raw sensor data but also the autonomous decisions of the smart contracts were secured in the ledger. In cases where the temperature value exceeded the determined maximum threshold (4°C), it was observed that the system automatically created a violation record (High Temp Violation), and this condition was irreversibly logged into the blockchain ledger. Due to the nature of distributed ledger technology (DLT), even the slightest manipulation attempt intended to be made subsequently on any recorded temperature data (e.g., falsely showing a lower temperature for a spoiled product) will instantly disrupt the mathematical cipher of that block and break the cryptographic link in the chain. Through this feature, the risk of retroactive data alteration, which is frequently encountered in cold chain logistics, is completely eliminated not only theoretically but also technically, thereby ensuring compliance with the principle of full transparency.

	Block_Index	Transaction_ID	Product	Temperature	SC_Risk	SC_Reason	Hash
0	1	TXN_103	Orange	36.15	Risk	High Temp Violation	[illegible]
1	2	TXN_436	Orange	12.52	Critical Risk	High Temp & Bad Quality	[illegible]
2	3	TXN_861	Pineapple	31.68	Critical Risk	High Temp & Bad Quality	[illegible]
3	4	TXN_271	Banana	6.4	Risk	High Temp Violation	[illegible]
4	5	TXN_107	Tomato	27.56	Risk	High Temp Violation	[illegible]
5	6	TXN_72	Orange	22.45	Risk	High Temp Violation	[illegible]
6	7	TXN_701	Pineapple	22.52	Critical Risk	High Temp & Bad Quality	[illegible]
7	8	TXN_21	Tomato	7.86	Critical Risk	High Temp & Bad Quality	[illegible]
8	9	TXN_615	Banana	11.53	Critical Risk	High Temp & Bad Quality	[illegible]
9	10	TXN_121	Pineapple	6.14	Risk	High Temp Violation	[illegible]

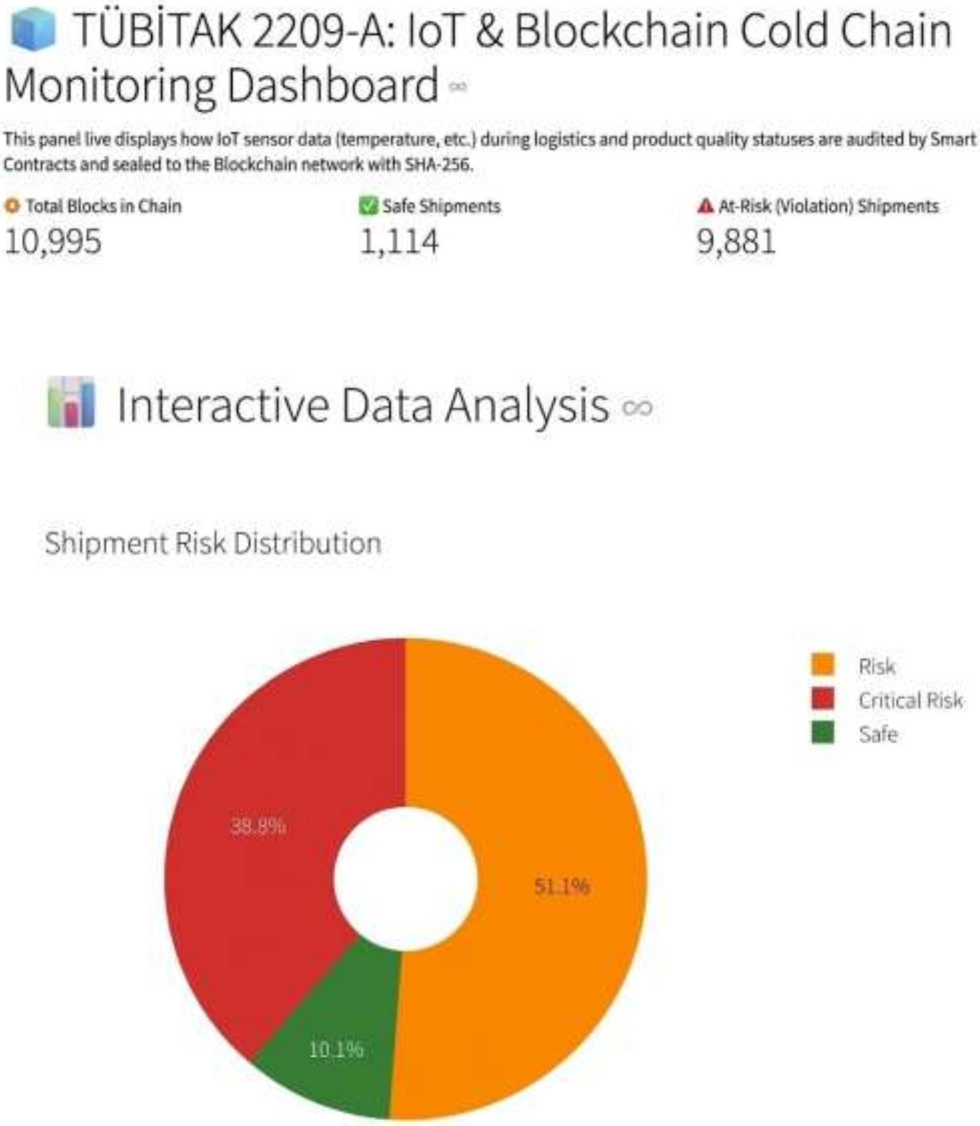
Figure 3. The blockchain ledger output encrypted with the SHA-256 algorithm.

D. *System Performance and Processing Time*

Transaction latency, which is one of the major drawbacks of blockchain networks in the literature, has been optimized in this project through the implemented lightweight encryption architecture. The analysis of the large logistics dataset consisting of 10,995 rows utilized in the system, its sealing with the SHA-256 algorithm, and its addition to the chain were completed within seconds. This confirmed that the established system can operate seamlessly in real-time, data-intensive industrial cold chain operations.

E. *User Interface and Filtering Performance (Web Dashboard)*

To present the autonomous system to end-users (logistics managers), an interactive Control Panel (Web Dashboard) was developed using the Streamlit framework (See Figure 4). During the interface tests, it was observed that "Risk" shipments could be filtered instantly from thousands of rows of encrypted data using dynamic filters, and the risk distribution was visualized without latency via a pie chart. This demonstrates that the project has advanced from a laboratory prototype to the level of a software product ready for commercialization.



TÜBİTAK 2209-A: IoT & Blockchain Cold Chain Monitoring Dashboard

This panel live displays how IoT sensor data (temperature, etc.) during logistics and product quality statuses are audited by Smart Contracts and sealed to the Blockchain network with SHA-256.

Total Blocks in Chain: 10,995

Safe Shipments: 1,114

At-Risk (Violation) Shipments: 9,881

Interactive Data Analysis

Shipment Risk Distribution

Figure 4. Interactive control panel (Dashboard) interface developed for data analysis and risk tracking.

IV. DISCUSSION

A. Comparison of the systemic approach with the literature

The IoT-based cold chain monitoring system developed within the scope of this study is an application-oriented study that focuses directly on hardware integration and data, unlike the theoretical approaches in the literature. When the literature is examined, for example, Ben-Daya et al. (2019) [12] addressed the transformative effects of IoT technologies on supply chain processes only in a conceptual and theoretical dimension, but excluded the integration of physical sensors to be used into the system and the evaluation of the accuracy and reliability of the data obtained from these devices. A similar deficiency is seen in the study by Rebelo et al. [14]. The application areas of physical sensors were excluded from the analyses. In this system we developed, we did not only limit ourselves to theoretical modeling, but also included hardware components in accordance with industrial standards in the process. The ESP32 microcontroller, which offers energy efficiency and network connectivity capacity, is positioned as the main management center. Physical environmental data obtained instantly from the field with DHT11 temperature and humidity sensors and GPS modules integrated into this unit are processed instantly, filling the hardware application gap seen in the literature. In the literature, Rejeb et al. While the large-scale bibliometric studies conducted by [13] outline the general features of the systems, the model we designed focuses directly on industrial applicability and cost-effectiveness. In particular, the fact that the system autonomously creates a breach record without any manual intervention or human approval when the defined thresholds, such as 4°C, which is a critical limit in cold chain logistics, are exceeded, distinguishes our project from traditional monitoring systems that only collect data. It transforms into a real-time control system that allows for the immediate detection and intervention of potential risks (Table 2).

Table 2. Technical comparison of the proposed hybrid model with traditional and solely IoT-based systems.

Parameter	Traditional Systems	Solely IoT-Based [10]	Proposed Hybrid Model
Data Security	Low (Manual Recording)	Medium (Central Database)	High (Immutable Blockchain)
Transparency	None	Limited	Full Transparency and Traceability
Intervention Speed	Very Low	High (Instant Notification)	High (Autonomous Smart Contract)
Cost	Medium	High	Low (ESP32-Based Prototype)

B. The impact of the blockchain layer on data integrity

As highlighted by Hussain et al. [9] in the literature, one of the major problems encountered in blockchain-based IoT systems is the lack of comprehensive analytical models in which data collected from physical sensors in the field is directly and seamlessly integrated with autonomous smart contracts. In traditional IoT infrastructures, storing and processing data collected from devices on centralized servers renders the entire system vulnerable to cybersecurity flaws, data manipulation, and the single point of failure (SPOF) risk, which can cause the system to collapse [9], [10]. The model developed in this study, however, eliminates these security risks by transferring the data collected from sensors directly to the blockchain layer built on the Ethereum test network.

When deviations from the predetermined temperature and humidity threshold values are detected, smart contracts protected by asymmetric encryption and robust consensus algorithms are instantly activated, autonomously recording the event. Thanks to this autonomous and decentralized structure, which replaces manual data recording and verification systems, human-induced errors that may occur during data entry and manipulation attempts aimed at concealing potential violations in the cold chain process (such as transporting products under inappropriate conditions) are rendered technically impossible. All occurring environmental changes and violation records are logged into a digital ledger that cannot be retroactively deleted or altered, thereby guaranteeing data integrity. Thus, the blockchain layer in our study acts not merely as a verification tool; it provides a transparent and secure infrastructure that is impervious to external tampering, effectively resolving trust issues among all stakeholders throughout the entire logistics process, from production to the final consumer.

V. CONCLUSION

In this study, a hybrid system model integrating IoT and blockchain has been developed to provide a solution to the data security, transparency, and traceability issues encountered in the logistics processes of highly temperature-sensitive products, primarily in the food and pharmaceutical sectors. Data manipulation and centralized server-induced security vulnerabilities, where traditional methods in cold chain logistics fall short, have been technically overcome by the decentralized structure and smart contract algorithms of the proposed system. Experimental studies and laboratory tests conducted within the scope of the project have proven that the real-time tracking of environmental parameters, the recording of data into the blockchain ledger in an immutable manner, and the autonomous alert mechanisms in the event of threshold exceedances operate successfully.

The results of the study are in strategic alignment with the "Zero Waste and Circular Economy" objectives within the scope of the "Green Deal Action Plan" published by the Ministry of Trade of the Republic of Türkiye in 2021. Thanks to the developed technological infrastructure:

By ensuring the preservation of the freshness of perishable products throughout the supply chain, it is aimed to prevent the economic loss and resource waste caused by the approximately 1.3 billion tons of food wasted annually on a global scale.

Through the capability of instant detection and intervention in temperature fluctuations during logistics processes, product losses are minimized, providing a concrete solution for reducing the carbon footprint and increasing energy efficiency.

The transparent tracking infrastructure provided by blockchain technology has strengthened trust protocols in the process from the producer to the final consumer and technically prevented counterfeiting risks.

In summary, the infrastructure we developed closes the critical data security gap in the cold chain sector. Because of this, it makes a direct and highly original contribution to the industry's digitalization. In summary, the infrastructure we developed closes the critical data security gap in the cold chain sector. Because of this, it makes a direct and highly original contribution to the industry's digitalization. We now have enough raw data from these trials to actually build predictive models. The whole idea is to stop reacting to temperature spikes and start anticipating them. If an AI module spots a risk, it will automatically change the route to save the cargo without needing human input. Turning this working prototype into a real-world product through the TEYDEB 1512 grant is our immediate priority. We are confident this will give Türkiye a serious competitive edge in cold chain logistics.

ACKNOWLEDGMENT

This study, under the application number 1919B012471097, was supported by the TÜBİTAK 2209-A University Students Research Projects Support Program. The authors would like to thank Fırat University for providing the laboratory facilities.

REFERENCES

[1] Precedence Research, "Cold Chain Market Size, Share, Growth Analysis, Trends, Report 2023-2032," 2023. [Online]. Available: https://www.precedenceresearch.com/cold-chain-market. [Accessed: Nov. 12, 2024].

[2] United Nations Environment Programme (UNEP), "Food Waste Index Report 2024," Nairobi, Kenya, 2024.

[3] S. Davoudi, P. Stasinopoulos, and N. Shiwakoti, "Two Decades of Advancements in Cold Supply Chain Logistics for Reducing Food Waste," Sustainability, vol. 16, no. 16, p. 6986, Aug. 2024.

[4] T.-h. Kim, V. S. Solanki, H. J. Baraiya, A. Mitra, H. Shah, and S. Roy, "A smart, sensible agriculture system using the exponential moving average model," Symmetry, vol. 12, no. 3, p. 457, 2020.

[5] S. Awan et al., "Blockchain ile loT: Tarım ve Gıda Tedarik Zincirinde Fütüristik Bir Yaklaşım," Kablosuz İletişim ve Mobil Bilişim, 2021.

[6] H. Erdoğan, K. Küçük, and S. A. Khan, "Endüstriyel IoT Bulut Uygulamaları için Düşük Maliyetli Modbus/MQTT Ağ Geçidi Tasarımı ve Gerçekleştirilmesi," Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Dergisi, vol. 7, no. 1, pp. 170-183, 2020.

[7] S. C. Mukhopadhyay et al., "Artificial intelligence-based sensors for next generation IoT applications: A review," IEEE Sensors Journal, vol. 21, no. 22, pp. 24920-24932, 2021.

[8] R. Jedermann and W. Lang, "Semi-passive RFID and beyond: steps towards automated quality tracing in the food cold chain," International Journal of Sensor Networks, vol. 24, no. 2, pp. 88-96, 2017.

[9] M. Hussain et al., "Blockchain-based IoT devices in supply chain management: A systematic literature review," Sustainability, vol. 13, no. 24, p. 13646, 2021.

[10] E. M. Torroglosa-Garcia, J. M. A. Calero, J. B. Bernabe, and A. Skarmeta, "Enabling roaming across heterogeneous IoT wireless networks: LoRaWAN MEETS 5G," IEEE Access, vol. 8, pp. 103164-103180, 2020.

[11] S. Tanwar, N. Gupta, C. Iwendi, K. Kumar, and M. Alenezi, "Next Generation IoT and Blockchain Integration," Journal of Sensors, vol. 2022, Article ID 9077348, 14 pages, 2022.

[12] M. Ben-Daya, E. Hassini, and Z. Bahroun, "Internet of things and supply chain management: A literature review," International Journal of Production Research, vol. 57, 2019.

[13] A. Rejeb, S. Simske, K. Rejeb, H. Treiblmaier, and S. Zailani, "Internet of Things research in supply chain management and logistics: A bibliometric analysis," Internet of Things, vol. 12, p. 100318, 2020.

[14] R. M. L. Rebelo, S. C. F. Pereira, and M. M. Queiroz, "The interplay between the internet of things and supply chain management: Challenges and opportunities based on a systematic literature review," Benchmarking: An International Journal, vol. 29, no. 2, pp. 683-711, 2022.

[15] Tempix. (n.d.). Soğuk Zincir Lojistiği. [Online]. Available: http://www.tempix.com.tr/sogukzincirlojistigi.html. [Accessed: Nov. 10, 2024].

[16] M. Xu, X. Chen, and G. Kou, "A systematic review of blockchain," Financial Innovation, vol. 5, no. 1, p. 27, 2019.

[17] A. I. Badran and M. Y. Kashmoola, "Smart agriculture using Internet of Things: a survey," in Proc. 1st Int. Multi-Disciplinary Conf. Theme: Sustainable Development and Smart Planning (IMDC-SDSP), 2020, p. 10.

[18] M. Z. Gündüz and R. Daş, "Nesnelerin interneti: Gelişimi, bileşenleri ve uygulama alanları," Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi, vol. 24, no. 2, pp. 327-335, 2018.

[19] R. Chataut, A. Phoummalayvane, and R. Akl, "Unleashing the power of IoT: A comprehensive review of IoT applications and future prospects in healthcare, agriculture, smart homes, smart cities, and industry 4.0," Sensors, vol. 23, no. 16, p. 7194, 2023.

[20] Blockchain Council, "Blockchain Council," [Online]. Available: https://www.blockchain-council.org. [Accessed: Mar. 17, 2026].

[21] Marius, Nshekanabo; Mugisha, Stanley (2025), “A Multi-Parameter Dataset for Machine Learning Based Fruit Spoilage Prediction in an IoT-Enabled Cold Storage System”, Mendeley Data, V1, doi: 10.17632/czz68d9fwj.1

[22] Programmer3, "Smart Logistics IoT Dataset," Kaggle, [Online]. Available: https://www.kaggle.com/datasets/programmer3/smart-logistics-iot-dataset. [Accessed: Mar. 15, 2026].