An RFID-Augmented Information Retrieval Technique for AI-Enabled IoT Devices Ensuring Agri-Food Traceability and Anti-Counterfeiting

Mohamed Riad Sebti, *Graduate Student Member, IEEE*, Alberto Arciello, *Graduate Student Member, IEEE*, Mariateresa Russo, and Massimo Merenda, *Senior Member, IEEE*

***Abstract*—Globalized agri-food supply chains face rising risks of traceability gaps and product fraud, especially during early production stages where environmental conditions affect safety and quality. This work introduces a compact and low-cost, power efficient MCU-based Edge-AI system that enhances real-time traceability and anti-counterfeiting from harvest to consumer. Environmental data are collected during harvesting, and the information saved into the RFID tag is generated directly from these data through an embedded AI model, enabling local, connectivity-free decision-making. The system is designed to run efficiently on microcontrollers, making it fully deployable in field conditions. The resulting information is securely stored in the RFID tag, which acts as a portable, tamper-evident data carrier. A dual-scan mechanism and backend anchoring ensure authenticity, while a blockchain layer provides immutable record-keeping in a simulated environment. A prototype applied to grape harvesting demonstrates high model accuracy, fast on-device inference, low power usage, reliable RFID operations, and ease of integration with a web-based traceability platform. These results show that combining Edge-AI with RFID and blockchain provides a scalable and practical solution for improving transparency and protecting agri-food products against counterfeiting.**

***Index Terms*—RFID, artificial intelligence, Internet of Things, agri-food, traceability, anti-counterfeiting.**

I. Introduction

With the rapid globalization of agri-food trade, ensuring product traceability, authenticity, and transparency across complex supply chains has become increasingly challenging [1]. Traceability plays a vital role in guaranteeing food safety, quality control, and regulatory compliance, yet maintaining it effectively across international and multi-actor supply chains remains difficult [2]. In the European Union, these requirements are formally established by Regulation (EC) No. 178/2002 [3], which defines food traceability as the ability to track and follow food, feed, and ingredients through all stages of production, processing, and distribution. Consumers today are more aware and concerned about the origin, quality, and composition of the food they consume, demanding greater confidence in labeling and certification processes [4]. However, the growing sophistication of counterfeit and adulterated products poses a serious threat to both public trust and market integrity [5]. High-value items such as Extra Virgin Olive Oil (EVOO) [6], honey [7], saffron [8], and wine [9] are particularly vulnerable, as counterfeit versions often mimic genuine products while being sold at premium prices despite not containing the expected natural components or quality standards. These fraudulent practices not only damage brand reputation and consumer confidence but also undermine the efforts of legitimate producers who adhere to strict quality and traceability requirements. Consequently, enhancing traceability and authenticity verification has become a central challenge for the agri-food sector in the era of globalized production and distribution [10]. Despite the growing use of digital technologies such as Radio Frequency Identification (RFID), Internet of Things (IoT), Blockchain (BC), and Artificial Intelligence (AI) [11], [12], [13] in the agri-food sector [14], existing solutions remain largely focused on the post-farm stages of the supply chain, including processing, logistics, and retail. Moreover, traceability can also be difficult to ensure in other stages of the supply chain. For example, during transportation, products such as dates that require strict cold-chain conditions may be exposed to unsuitable temperatures, causing a loss of quality [15], [16]. As a result, the quality estimated during earlier stages may not reflect the actual condition of the product that reaches consumers or other stakeholders, potentially harming brand reputation and reducing trust. In contrast, the farm stage—where environmental conditions, cultivation practices, and data variability are most critical—still lacks reliable and cost-effective digital solutions. This is particularly concerning in cases such as grape harvest, where variations in temperature

Received 18 November 2025; revised 14 January 2026; accepted 7 February 2026. Date of publication 11 February 2026; date of current version 20 February 2026. This work was supported by European Union (EU) Next-GenerationEU, National Recovery and Resilience Plan (PNRR)–Missione 4-Componente (M4C2)–Investment 1.5–"Innovation Ecosystems," through the project "Ecosistema TECH4YOU–Technologies for Climate Change Adaptation and Quality of Life Improvement" D.D. 3277 (30 December 2021). *(Corresponding author: Massimo Merenda.)*

Mohamed Riad Sebti is with the DIIES Department and the FOCUSSLab, Mediterranea University of Reggio Calabria, 89124 Reggio Calabria, Italy (e-mail: riad.sebti@unirc.it).

Alberto Arciello is with the DIIES Department, Mediterranea University of Reggio Calabria, 89124 Reggio Calabria, Italy (e-mail: alberto.arciello@unirc.it).

Mariateresa Russo is with the FOCUSSLab, Mediterranea University of Reggio Calabria, 89124 Reggio Calabria, Italy (e-mail: mariateresa.russo@unirc.it).

Massimo Merenda is with the DIIES Department, Mediterranea University of Reggio Calabria, 89124 Reggio Calabria, Italy, and also with HWA Srl Spin-off, Mediterranea University of Reggio Calabria (UNIRC), 89126 Reggio Calabria, Italy (e-mail: massimo.merenda@unirc.it).

Digital Object Identifier 10.1109/JRFID.2026.3663762

and humidity can lead to the potential growth of Ochratoxin A (OTA) [17], [18], [19], a toxic secondary metabolite produced by certain fungal species. OTA poses serious health risks to consumers and can cause substantial economic losses in wine, juice and grape production. Its presence is strictly regulated by the European Union [20], making early detection and monitoring of environmental factors at the farm level a crucial aspect of food safety and quality assurance. This absence of on-field traceability and monitoring tools creates a significant information gap at the very beginning of the supply chain, where product quality and authenticity are first established. Moreover, most current traceability systems rely on centralized architectures for data transmission and storage, which exposes them to potential data manipulation or inconsistency between different stages. As a result, ensuring the integrity and authenticity of data collected at the farm level remains a major challenge, particularly in low-connectivity or resource-constrained environments. To address these limitations, this paper proposes a low-cost RFID-enabled Edge-AI framework designed to ensure secure and real-time traceability in agri-food supply chains. The proposed system integrates affordable sensors with an intelligent Microcontroller unit (MCU) capable of performing on-device inference using an embedded AI model. This approach reduces the need for continuous cloud connectivity and minimizes the volume of transmitted data, making it suitable for deployment in remote and resource-constrained farm environments. The inferred data are securely written to passive RFID tags, which serve as portable and tamper-evident data carriers, and subsequently logged onto a simulated BC demonstrating the feasibility of immutable record-keeping and anti-counterfeiting verification within a controlled environment. In addition, a web-based interface was developed to allow stakeholders and consumers to access and verify product information via QR Code, enhancing transparency and trust across the supply chain. To demonstrate the system's feasibility, a case study is conducted in a laboratory environment using grape farm data firstly presented in [19], representing a challenging traceability scenario characterized by environmental variability and limited technological infrastructure.

The main contributions of this paper can be summarized as follows:

1) Integration of Edge-AI and RFID for on-product intelligence, enabling real-time inference and secure storage of analytical results directly in RFID tags.
2) Low-cost and autonomous Edge-AI architecture performing sensing, inference, and traceability locally at the farm level to reduce cloud dependency.
3) Compact RFID encoding and dual-scan mechanism provides best-effort authenticity, tag integrity, and resistance to counterfeiting.
4) Experimental validation on grape farm data, confirming the system's feasibility and robustness under realistic agricultural conditions.

The remainder of this paper is organized as follows: Section II provides a detailed analysis of the state-of-the-art, reviewing implemented solutions for traceability and anti-counterfeiting in the agri-food sector. It highlights the main challenges and limitations of current approaches and outlines how the proposed framework overcomes these issues through the integration of Edge-AI and RFID technologies. Section III describes the methods used to design and develop the proposed framework. Section IV presents the implementation details, including the setup, AI model integration, and system workflow. Section V reports and analyzes the experimental results obtained from the farm-level deployment. Section VI discusses the main findings of the study, analyzes the identified security threats and corresponding mitigation strategies, and outlines the current system limitations. Finally, Section VII concludes the paper and provides future perspectives for expanding the system's applicability in broader agri-food contexts.

II. State-of-the-Art Solutions and Architectural Paradigms

Over the past two decades, the architectures of agri-food traceability and anti-counterfeiting systems have evolved through successive technological generations aimed at increasing transparency, data reliability, and automation across the supply chain. Initially, RFID-based systems emerged as one of the earliest enablers of digital traceability, providing a means to uniquely identify and monitor products without manual scanning or line-of-sight requirements [21]. These systems represented a fundamental shift from paper-based documentation toward electronic and sensor-assisted data collection. For instance, Amador et al [22] demonstrated how RFID temperature tags could be deployed along the pineapple supply chain to monitor temperature fluctuations during transport and storage, achieving accuracy comparable to conventional methods while greatly improving data accessibility and instrumentation efficiency. Similarly, another RFID-enabled framework introduced automated tagging and data capture mechanisms for quality control in perishable goods, showing that RFID sensors could significantly enhance product monitoring and logistical efficiency across food networks [23]. These studies collectively underscored the potential of RFID for traceability but also revealed its limitations, most notably, the dependence on costly active tags and the absence of integrated data analytics or dynamicity across distributed nodes. The introduction of the IoT marked a major shift toward automated and sensor-driven traceability in agri-food systems. IoT-based architectures enable continuous monitoring and data acquisition from the field, improving transparency and responsiveness along the supply chain. Corallo et al. proposed a multilayer IoT framework combining sensor, business process, and application layers to ensure interoperability and data sharing across stakeholders [24]. Wongpatikaseree et al. developed a smart farm system that integrates environmental sensing, cloud data management, and QR-based consumer traceability [25]. These approaches demonstrated the potential of IoT for real-time monitoring and consumer engagement, though their dependence on stable internet connectivity and centralized data storage limits scalability in rural environments. The combination of AI with IoT has introduced a new generation of intelligent traceability systems capable of autonomous data analysis and adaptive decision-making. AI-integrated IoT architectures extend conventional sensing

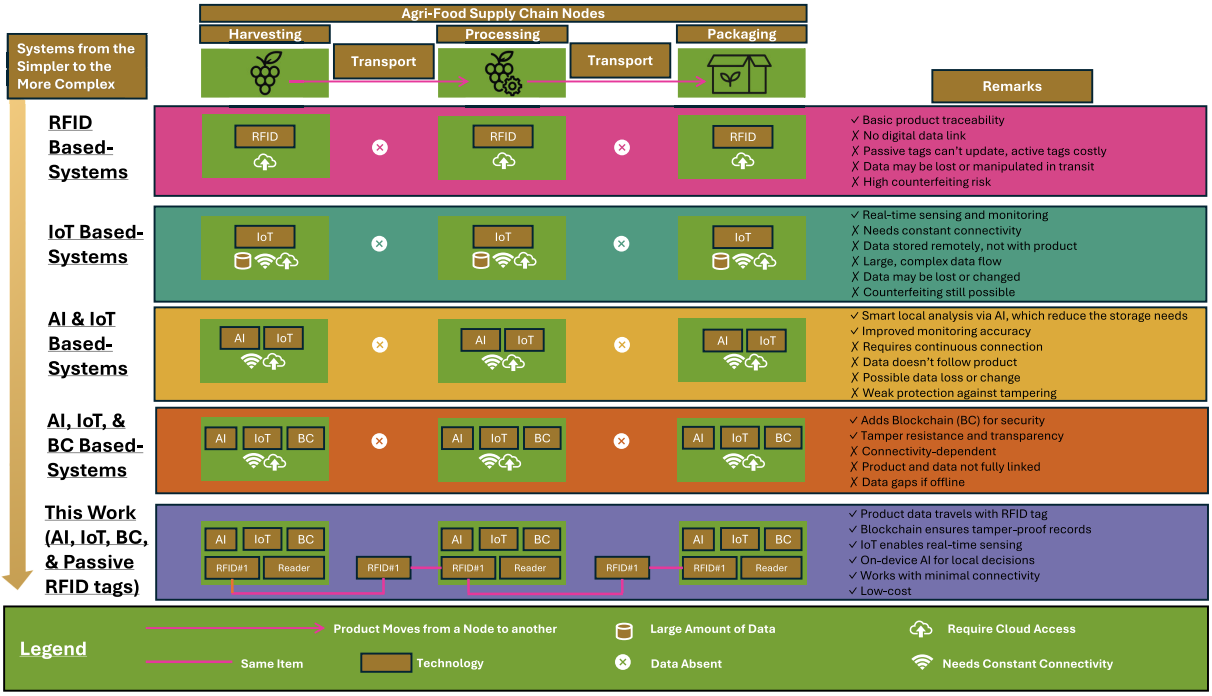


Fig. 1. Comparative overview of agri-food traceability architectures.

networks by embedding learning models directly into edge or cloud layers [26], allowing for predictive and prescriptive capabilities in agricultural operations. In one implementation, Machine Learning (ML) models were integrated into an IoT-based monitoring platform to classify crop conditions and detect anomalies from environmental data streams, improving resource management and early stress identification [27]. Similarly, Bhatta and Natarajan proposed an AI–IoT framework employing drones, neural networks, and image processing to assess crop health and automate field interventions [28]. These systems illustrate how coupling AI with IoT enhances situational awareness and operational efficiency. However, they still depend on substantial computational resources and reliable network access for model updates and data synchronization, posing challenges for low-cost or remote agricultural deployments. In addition to AI and IoT, several recent systems have adopted BC to further enhance data integrity and transparency in agri-food traceability. The integration of AI, IoT, and BC (AI–IoT–BC) technologies represents the most advanced paradigm, combining intelligent data analytics with decentralized and tamper-proof storage. These hybrid architectures enable transparent, autonomous, and privacy-preserving data exchange among stakeholders while ensuring that sensing and decision-making processes remain verifiable. Gaudio et al. proposed a multi-layered solution that interconnects IoT devices, AI-based data selection, and Hyperledger Fabric to achieve secure and scalable traceability across food chains [29]. Their system employs permissioned BC nodes linked to IoT clusters that collect and pre-process data, while an AI layer filters relevant information before committing transactions to the ledger, reducing network load and improving efficiency. Likewise, Kumar et al. developed an integrated AI–IoT–BC architecture for smart agriculture that enhances data security, optimizes farm operations, and supports real-time decision-making through predictive analytics [30]. Despite these advances, current AI–IoT–BC solutions often require constant connectivity, continuous cloud access, and the recorded information does not physically follow the product as illustrated in Fig. 1. Building upon these advancements, the system proposed in this work introduces a more practical, low-cost, and resilient architecture that integrates AI, IoT, simulated BC, and passive RFID tags to achieve continuous, product-linked traceability across the entire agri-food supply chain. Unlike previous paradigms where digital information remains detached from the physical product, this design ensures that data physically follow the product through RFID identifiers embedded at each node. Real-time environmental sensing is performed locally through IoT devices, while on-device AI enables immediate classification of the collected data, supports autonomous decision-making at the edge, and optimizes memory usage by writing only the resulting label—representing a condensed summary of multiple sensed parameters—to the RFID tag instead of storing the full dataset. In the current implementation, the user memory of each RFID tag was written once during harvesting, however, the architecture also supports multi-write operations, either by selectively overwriting fields or by continuing new data from the last written address (for example: if the first write occupies 100 characters, the next begins at 101). Because passive UHF tags have limited write cycles, overwriting is minimized, and versioning metadata will be introduced to prevent rollback. The simulated BC layer serves as a proof-of-concept for secure, tamper-evident data recording and verifiable provenance across supply chain nodes.

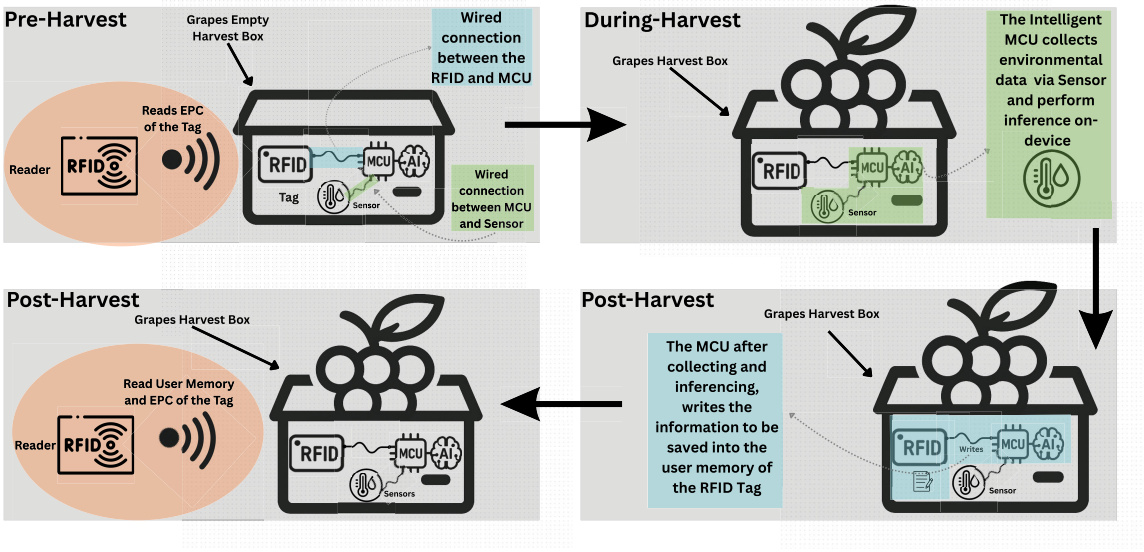


Fig. 2. Workflow of the proposed RFID–Edge-AI system during the harvest process.

III. Methods

This study builds upon our previously published work on real-time OTA contamination detection in grapes [19], which established an AI–IoT framework for environmental-based mycotoxin risk assessment. The current work extends that system by integrating RFID technology and a simulated BC layer to achieve secure, product-linked traceability and anti-counterfeiting. Additionally, the hardware setup was updated by replacing the M5StickC plus (M5C+) MCU used in the previous study with another MCU offering more wiring options. This change allows for the connection of multiple sensors and peripherals simultaneously, overcoming the limited I/O capabilities of the M5C+. It also facilitates more stable model embedding and inference execution directly on the device, thereby improving performance and reliability under real deployment conditions. While the earlier OTA-oriented implementation focused primarily on chemical analysis and data validation, the present study advances this architecture toward end-to-end traceability, ensuring that the collected data remain verifiable, traceable, resistant to counterfeiting, accessible in real time, securely recorded on the BC, and physically associated with each product through RFID tags.

A. System Architecture

The proposed system is designed to enhance traceability and anti-counterfeiting at the farm level, where the supply chain is most vulnerable to information gaps and manipulation. The architecture targets the grape harvest process, spanning pre-harvest, harvest, and post-harvest phases, and culminating in consumer verification. Fig 2 illustrates the overall workflow during the harvest process. The system integrates five main components: (i) an edge device with embedded intelligence, (ii) RFID-enabled harvest boxes, (iii) a BC-secured backend, (iv) a web application, and (v) a QR-code verification mechanism. At the edge layer, an MCU equipped with environmental sensors captures temperature, humidity, and harvest duration during the harvest process. A lightweight ML model deployed directly on the MCU processes these data locally to classify potential risk of OTA contamination, which serves as the use case in this implementation. The same architecture, however, can support different embedded-AI tasks depending on the targeted use case, the available data, and the deployed model. This ensures that reliable information is captured at the point of origin, limiting the possibility of falsification at later stages. Each harvest box is equipped with an RFID tag that acts as a secure memory unit. The tag's Electronic Product Code (EPC) functions as the unique key for traceability. The EPC is scanned twice during the workflow: once at the start of the harvest process to initialize a harvest session, and once at the end to ensure that results are bound to the correct product unit. Although the system relies mainly on EPC-based identification, the tag's immutable Tag Identifier (TID) can also be considered as an additional hardware-level reference to strengthen protection against tag cloning [31]. At the completion of harvest, summarized results are written into the tag's user memory, embedding essential supply chain information directly into the physical product. The RFID reader bridges the edge and backend layers by scanning both EPC and user memory content and uploading the full record of each box. The backend manages data storage and anchors cryptographic hashes of records onto a BC layer to guarantee immutability and detect tampering. A web application (AgriTraceX) enables stakeholders to visualize harvest records, monitor conditions linked to each box or batch via QR codes. Scanning the QR code allows consumers and regulators to verify authenticity and access the traceability history, ensuring transparency from vineyard to market. In summary, the architecture ensures that each harvested box is uniquely identified through its EPC, that environmental and risk classification data are directly tied to the physical product, and that all records are secured through BC anchoring. By combining embedded AI, RFID, BC, and QR-code verification, the system strengthens traceability while reducing opportunities for counterfeiting in the grape supply

chain. In this context, data are the raw Sensor readings collected during harvesting, while information represents the processed results written into the RFID tag.

B. Hardware

The proposed system relies on a set of lightweight and portable hardware components that can be easily deployed in the field. The core elements are summarized as follows:

- SHT40 Sensor: a digital temperature and humidity sensor used to monitor environmental conditions during harvest.
- Arduino Nano 33 BLE: the MCU is used as the edge computing device [32]. It integrates an ARM Cortex-M4 processor with 1 MB flash and 256 KB RAM, and supports Bluetooth Low Energy connectivity. In this work, the MCU is responsible for acquiring environmental data from sensors, executing the quantized TensorFlow Lite model for OTA risk classification, and writing the inference summary into the passive RFID tag. The board was powered via USB and an external battery during the experiments, however, future implementations will employ an integrated battery to enable fully autonomous operation in the field also exploiting renewable energy recharging systems.
- RFID Tag (EM4325): the harvest box is equipped with an EM4325 passive UHF RFID tag. The tag includes a unique EPC for product identification and additional user memory used in this system to store AI-generated information. Although it primarily operates in passive UHF mode, it can also function in semi-passive mode when externally powered, enabling repeated write operations to the user memory.
- Wired interface between MCU and sensor: a wired I^2C connection between the Arduino Nano 33 BLE and the SHT40 sensor enables the MCU to acquire temperature and humidity data in real time. The sampling interval can be adjusted according to the use case, ranging from every 30 minutes to every 6 hours [19], ensuring flexible and reliable data collection from the sensing unit to the edge device.
- Wired interface between MCU and RFID Tag: a wired connection between the Arduino Nano 33 BLE and the EM4325 tag allows the MCU to perform read and write operations on the user memory. This integration ensures that the information generated on-device can be securely stored directly on the tag.
- RFID Antenna and Reader (Universal Reader Assistant): during system development and testing, a fixed antenna connected to an RFID reader was employed together with the Universal Reader Assistant software. This setup was used to validate EPC scanning, user memory access, and MCU-tag communication before full deployment.
- ORCA-50 Handheld Data Terminal: for operational use, an ORCA-50 handheld RFID terminal [33] was employed to read EPC codes and user memory from the harvest boxes. The device also provides wireless connectivity, allowing information to be uploaded to the backend system where it is stored and anchored on the BC.

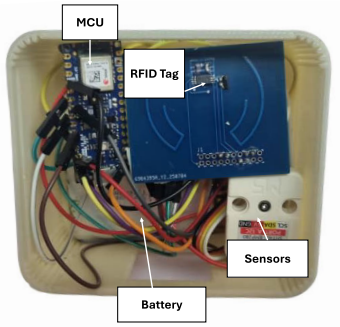


Fig. 3. Prototype setup showing the Arduino Nano 33 BLE, SHT40 Sensor, EM4325 RFID tag, and the battery placed behind the sensor.

The integration of the tag, MCU, sensor, and battery within the prototype setup is shown in Fig 3. In this configuration, the battery is positioned behind the sensor, while the other components are arranged to ensure compact wiring and portability in a Proof-of-Concept fashion.

C. Software

The software stack integrates edge intelligence, embedded development, cloud services, and web technologies to support reliable traceability and anti-counterfeiting throughout the grape supply chain. The workflow begins with model development, where a lightweight risk-assessment model was trained in Python using Google Colab. The model was subsequently quantized with TensorFlow Lite to reduce its computational footprint and enable efficient execution on MCU-class devices. On the embedded side, the quantized model was deployed on the Arduino Nano 33 BLE and programmed through the Arduino IDE. The MCU executes the embedded inference engine, continuously acquires sensor measurements, and processes them in real time. At predefined intervals, the firmware writes the resulting analytical output into the user memory of the EM4325 RFID tag. Although the sensor, MCU, and tag are physical components, the behaviour orchestrating data acquisition, on-device inference, and RFID memory updates is fully controlled through custom firmware, which represents a core element of the software stack. The reader application was developed in Android Studio for the ORCA-50 handheld terminal. This mobile application manages EPC and user-memory scanning, performs data formatting, and uploads harvested information to the backend. All harvest records are stored in Supabase, which provides a managed PostgreSQL database, user authentication, and serverless functions used to enforce secure access control and real-time synchronization. Finally, a full-stack web application—AgriTraceX—was built using React 18, TypeScript, and Tailwind CSS. This interface enables stakeholders to explore harvest records, inspect historical measurements, and generate QR codes for consumer verification. The web frontend interacts with the Supabase backend, while the QR-code mechanism provides an accessible means for customers and regulators to verify product authenticity directly from the field to the market. Overall, the software architecture spans embedded firmware, Android development, cloud storage, and a web-based visualization

layer, collectively enabling a complete digital traceability pipeline.

D. Embedded AI Model

This subsection presents the embedded AI module integrated within the proposed traceability framework. The model estimates the risk of ochratoxin A (OTA) contamination in grape harvest environments using real-time environmental data. It builds upon our previous work [19], where a data-driven OTA risk estimation model was derived from chemical analysis and environmental measurements. In this study, the model is adapted for integration with the RFID-based traceability system, enabling automatic recording of OTA risk levels directly into the tag memory during data collection.

1) Chemical Analysis and OTA Quantification: as detailed in our previous study [19], a chemical analysis was performed to establish the relationship between ochratoxin A (OTA) accumulation and environmental parameters during grape harvest. The experimental results revealed a strong dependence of OTA concentration on temperature, relative humidity, and harvest time. From these observations, an empirical function linking temperature (T), humidity (H), and harvest duration (t) to OTA concentration was derived and subsequently used to generate ground-truth labels for supervised model training. This function formed the analytical foundation for the OTA risk classification adopted in this work. Although this empirical function provides a deterministic relationship between (T, H, t) and OTA concentration, our previous analytical and experimental study [19] demonstrated that OTA formation follows exponential and threshold-driven fungal growth dynamics as a function of temperature, humidity, and harvest duration. These nonlinear interactions cannot be reliably captured by multilinear regression models. For this reason, a neural classification model is adopted to learn these complex dependencies from data and to provide robust, multi-class OTA risk estimation from real-time environmental measurements.

2) Task and Model Inputs: the OTA risk assessment task was formulated as a multi-class classification problem. The input vector $\mathbf{x} = [T, H, t]$ contains environmental features collected during harvest, namely temperature (T), relative humidity (H), and elapsed harvest time (t).

3) Model Architecture and Training: the same lightweight multilayer neural network previously deployed on the M5c+ device [19] was adopted for the Arduino Nano 33 BLE implementation. The network consists of two fully connected hidden layers with ReLU activation and an output layer with five neurons, each corresponding to one OTA risk class. A softmax activation function produces the probability distribution across the classes. The model was trained in Python on Google Colab for 250 epochs using the Adam optimizer, then converted to TensorFlow Lite, followed by quantization for execution with TFLite Micro on the MCU.

4) Multi-Class Formulation: the classification task was defined with reference to real-world production criteria. Commission Regulation (EC) No. 1881/2006 [34] establishes a maximum OTA level of 2 μg/kg for wine and grape juice, providing a binary distinction between acceptable and unacceptable batches. While this binary threshold is suitable for regulatory enforcement, it lacks the granularity needed for decision-making during harvest and early supply chain stages. To address this, the OTA risk range was subdivided into five classes, as shown in Table I. Specifically, Class 0 represents safe levels, Class 1 indicates low risk, Class 2 corresponds to moderate risk, Class 3 captures high but borderline levels, and Class 4 represents critical contamination above the legal limit. In this scheme, Classes 0 and 1 are considered acceptable for production and labeled as acceptable quality, whereas Classes 2, 3, and 4 are classified as unacceptable, corresponding to OTA concentrations above the regulatory threshold. For practical traceability purposes, all batches belonging to Classes 2–4 automatically activate a red-flag indicator, which is encoded in the RFID tag's user memory to support preventive actions such as segregation or rejection of contaminated batches. The OTA classifier was trained and evaluated on a limited dataset collected from a single grape cultivar under controlled harvesting conditions. The five-class risk categorization described above was derived from this dataset to represent varying OTA contamination levels. While the model achieved satisfactory performance within these conditions, its generalization to other cultivars, microclimates, or harvest seasons is not yet validated. Future work will extend the dataset to multiple grape varieties and environmental settings to assess robustness and adaptability.

TABLE I
OTA RISK CLASSIFICATION SCHEME [19] BASED ON COMMISSION REGULATION (EC) NO. 1881/2006 [34]

Class	Range (μg/kg)	Concentration	Quality	Red-Flag
0	0–1.0	Near zero	Acceptable	No
1	1.0–2.0	Low	Acceptable	No
2	2.0–3.0	Moderate	Unsafe	Yes
3	3.0–4.0	High	Unsafe	Yes
4	>4.0	Critical	Unsafe	Yes

E. BC Integration for Traceability

To ensure the integrity and traceability of supply chain records, a private simulated BC layer was integrated into the AgriTraceX platform. Each transaction is hashed using a lightweight JavaScript-based function and appended to a chain of blocks, where each block contains an index, timestamp, transaction data, and the hash of the previous block. The chain is initialized with a genesis block representing the initial product registration. This hash-chaining mechanism guarantees data immutability, as any tampering becomes immediately detectable. BC data is stored in a PostgreSQL database (Supabase), while the BC structure is dynamically generated for verification and consumer-facing queries. Although the system operates in a centralized environment without distributed consensus, it effectively demonstrates key BC properties—immutability, transparency, and auditability—thus ensuring reliable traceability across the agri-food supply chain.

IV. IMPLEMENTATION

To realize the architecture described in Section III-A, a laboratory prototype was developed and validated. Fig 4 illustrates the overall system architecture.

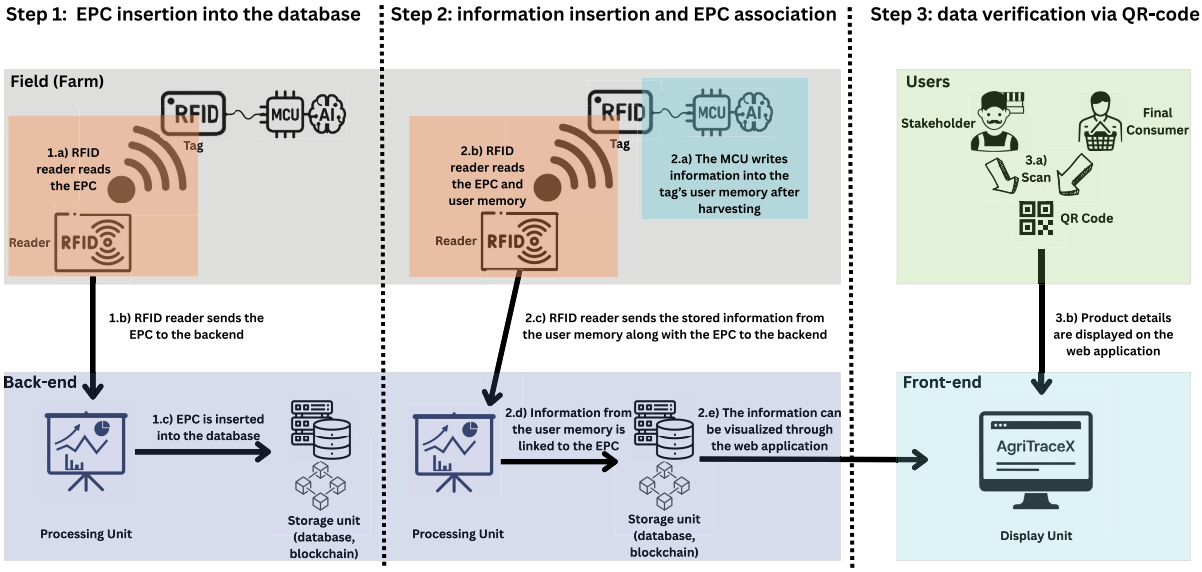


Fig. 4. Overall system architecture.

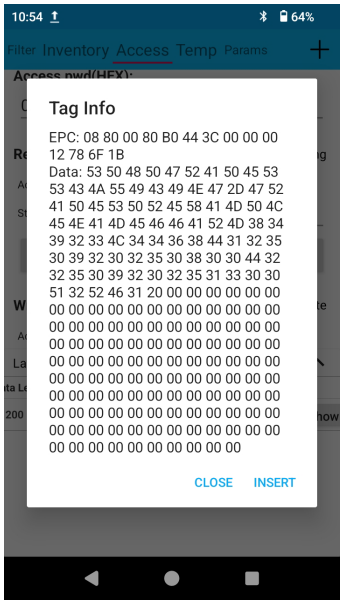


Fig. 5. Screenshot from the mobile reader application.

TABLE II
WIRING CONFIGURATION BETWEEN MCU, SENSOR, AND RFID TAG

Interface	Signal	Function
I^2C (Sensor–MCU)	SDA	Data line for communication.
	SCL	Clock line for synchronization.
	3V3	3.3 V power supply.
	GND	Common ground.
SPI (RFID Tag–MCU)	MISO	Tag → MCU data transfer.
	MOSI	MCU → Tag data transfer.
	SCLK	Serial clock signal.
	CS	Chip select for tag activation.
	VDD	Power supply for tag.
	GND	Common ground.

Prior to system operation, the OTA risk classification model was trained in Python and converted into a quantized

TABLE III
ENCODING OF SUPPLY CHAIN AND HARVEST DATA STORED IN THE EM4325 RFID USER MEMORY

Code	Example	Description	Size (chars)
V	V01	Payload version	2
S	PH	Stage (e.g., PH = Post-Harvest)	2
P	Grapes	Product type	12
SC	juicing-Grapes	Supply chain type	20
PR	ExampleName	Producer	12
F	Farm84923	Farm ID	12
L	4468	Lot number	6
D1	250920250800	Harvest start (DDMMYYYYHHMM)	12
D2	250920251300	Harvest end (DDMMYYYYHHMM)	12
Q	0/1/2	Quality (0 = good, 1 = mid, 2 = bad)	1
RF	0/1	Red-flag (1 = flagged, 0 = safe)	1
DM	RESERVED	Reserved field for future metadata	2+ 292 (the rest)
Example	*V01SPHPGRAPESSCJUICING-GRAPESPREXAMPLENAMEFFARM84923 L4468D1250920250800D2250920251300Q2RF1DM*		92

TensorFlow Lite version suitable for deployment on resource-constrained devices. The quantized model was embedded into the Arduino Nano 33 BLE MCU, enabling local inference without requiring network connectivity. As illustrated in Fig. 4, the system operation consists of three main steps. In Step 1, the RFID reader scans the EPC of the EM4325 tag attached to an empty harvest box (Step 1.a). This EPC acts as a unique digital identifier for traceability throughout the supply chain. The reader then transmits the scanned EPC to the backend (Step 1.b), where it is stored in the database and linked to a new BC record (Step 1.c). At this stage, the backend—composed of the processing unit and storage unit (database and BC)—initializes the product entry, ensuring that every box has a unique traceable identity prior to harvest. The RFID reader is controlled through a dedicated mobile application, which provides an intuitive interface for scanning EPCs, reading the user memory, and automatically uploading the retrieved information to the backend in real time via Wi-Fi or mobile network connectivity. In Step 2, during the harvesting process, the Arduino Nano 33 BLE periodically acquires temperature, humidity, and time data through an SHT40 sensor connected via an I^2C interface (SDA, SCL, 3V3, GND). The wiring configuration of the interfaces used

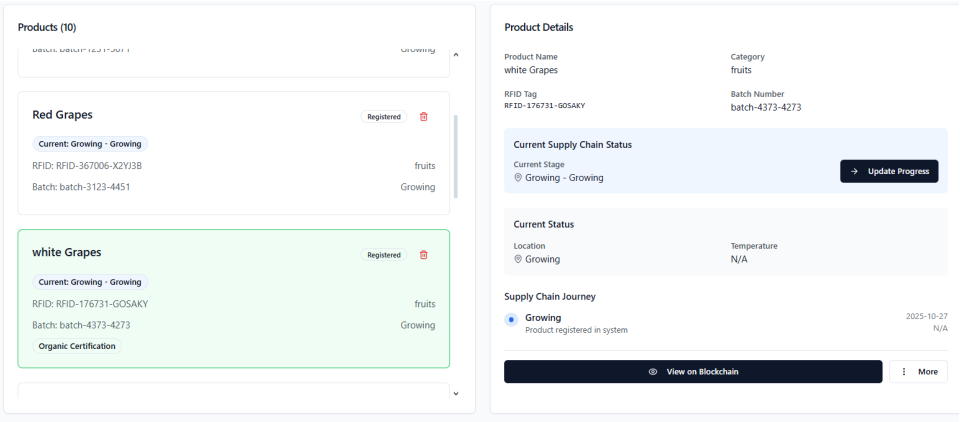


Fig. 6. AgriTraceX front-end displaying product registration and supply-chain tracking information linked to RFID tags.

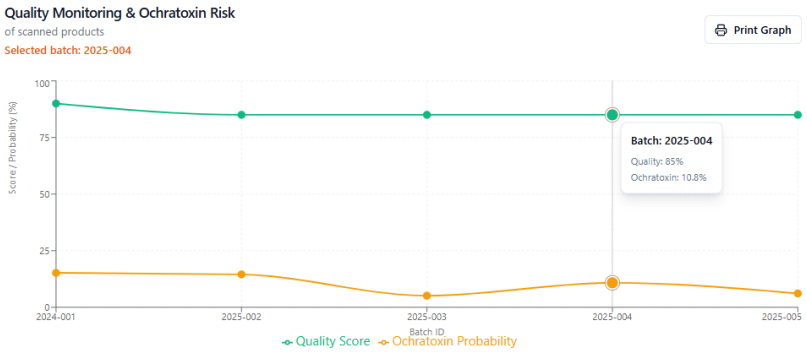
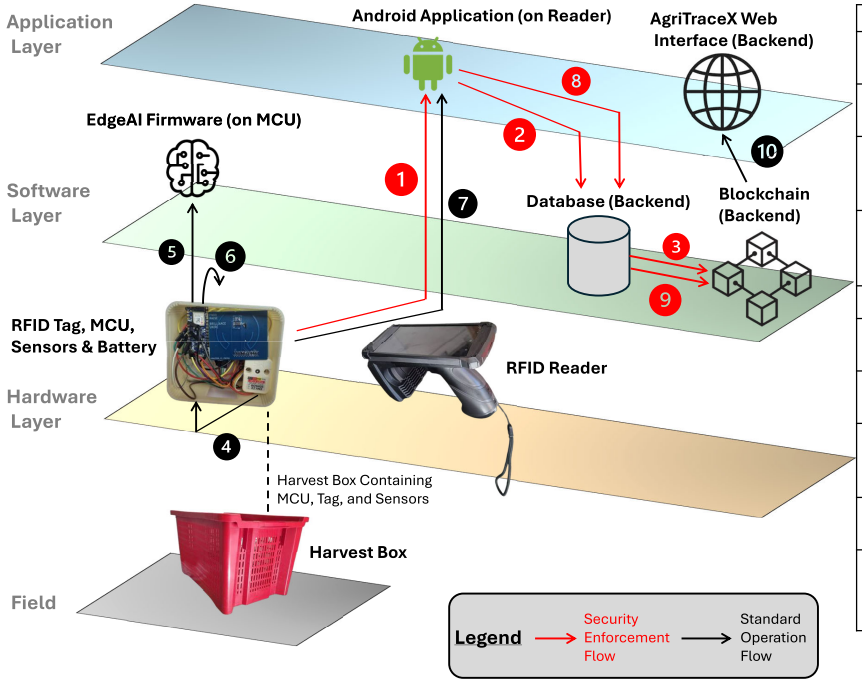


Fig. 7. Ochratoxin risk visualization on the web.



	Action
1	Acquire the EPC from the RFID Tag using the Reader
2	Insert the acquired EPC into the database
3	Log the first EPC insertion into the Blockchain to ensure secure registration
4	Measure environmental data via Sensors which are collected from the MCU
5	Perform on-device AI inferencing
6	Write the processed and essential information into the user memory
7	Retrieve information from the RFID tag through the Reader
8	Compare the verified EPC with the first registered EPC and link the newly retrieved information
9	Log the verified information into the blockchain
10	Display the blockchain-verified information on the AgriTraceX web interface

Fig. 8. Layered architecture of the framework.

for communication between the MCU, the sensor, and the RFID tag is summarized in Table II. The embedded AI model performs on-device inference at each sampling interval on these data to generate meaningful information, estimating

OTA risk based on real-time environmental conditions. During harvesting, the MCU wakes up every 30 minutes to execute this sensing–inference cycle and overwrites the RFID user memory with the newly generated result, ensuring that only the most recent and relevant information is retained by the end of the harvesting process. At the end of harvesting, the last 30-minute update corresponds to the final OTA risk classification and metadata stored in the RFID user memory via the SPI interface (MISO, MOSI, SCLK, CS, VDD, GND) (Step 2.a). The RFID reader then performs a second scan to read both the EPC and the updated user memory (Step 2.b) and transmits these information to the backend (Step 2.c). In the backend, the received user memory content is linked to the corresponding EPC (Step 2.d), and the complete record is stored and anchored on the BC to ensure immutability and provides best-effort authenticity. To facilitate on-site operations, the RFID reader is paired with a custom Android application that handles EPC scanning, user memory access, and backend synchronization. The interface of the reader application is shown in Fig. 5. The screen displays the raw tag data, including the EPC and the hexadecimal user memory content. Finally, the processed data (information) are synchronized with the AgriTraceX web application (Step 2.e), making them available for visualization and audit. The AgriTraceX front-end (Fig. 6) provides a user interface for registering products, visualizing their traceability status, and verifying OTA risk information stored in the database. In Step 3, data verification is performed via a QR code that can be attached to the product from the very first stage of the supply chain. Stakeholders and final consumers can scan the QR code using a smartphone (Step 3.a) to retrieve the corresponding BC-verified record, which displays all relevant product details—such as producer ID, harvest date, quality classification, and OTA risk level—on the web interface (Step 3.b). This ensures complete end-to-end traceability from field data capture to consumer transparency. Due to the limited 384-character capacity of the EM4325 tag's user memory, a compact encoding format was implemented. Each information field is represented by a short prefix (e.g., "V" for versioning, "S" for stage, "P" for product, "D1" for harvest start date). The encoded string, such as "V01SPHPGRAPESSCJUICING-GRAPESPREXAMPLENAME FFARM84923L4468D1250920250800D2250920251300 Q2RF1DM" contains essential attributes including product type, producer ID, farm, lot number, harvest time, OTA risk class, and red-flag indicator, as summarized in Table III. This structure ensures that critical traceability information physically accompanies the product while maintaining lightweight data storage and efficient backend integration. The OTA probability visualization for a scanned product is shown in Fig 7. The dashboard provides a clear representation of the OTA contamination risk and overall product quality score. Each data point corresponds to a specific product batch, with interactive tooltips displaying detailed attributes such as batch ID, quality percentage, and OTA probability. This visual interface allows stakeholders to monitor product quality trends and potential contamination risks directly from the AgriTraceX web platform. The integration between the material, hardware, software, and application layers of the implemented prototype is summarized in Fig. 8, providing an overview of the complete traceability flow from sensor data collection to visualization.

TABLE IV
FINAL MODEL PERFORMANCE EVALUATION

Metric	Value (%)
Train Accuracy	97.28%
Validation Accuracy	98.55%
Test Accuracy	96.53%

TABLE V
ON-DEVICE RESOURCE UTILIZATION ON ARDUINO NANO 33 BLE SENSE

Resource	Usage	Maximum Available
Flash	365,800 bytes (37%)	983,040 bytes
RAM	127,832 bytes (48%)	262,144 bytes

V. RESULTS AND PERFORMANCE

A. On-Device Implementation

1) Model Performance: the deployed model demonstrated strong predictive capability after quantization and deployment to the embedded platform. Its performance remained consistent with the results obtained during the training and evaluation phases, indicating that the optimization and conversion steps did not lead to significant degradation. The final accuracy metrics are summarized in Table IV, showing that both training and validation phases achieved high performance, while the test accuracy remained above 96%, confirming the suitability of the model for real-time inference on resource-constrained devices.

2) Inference Time: the real-time inference capabilities of the deployed AI-model were evaluated to assess its suitability for continuous decision-making on resource-limited hardware. Each inference operation, executed immediately after sensor data acquisition, required less than 1 ms. More precisely, the measured latency ranged between 650 and 700 μ s per prediction. Such low latency demonstrates the ability of the system to operate in real time while maintaining high responsiveness for downstream tasks, including RFID tag updates and communication processes.

3) Resource Utilization: the on-device data flow, where sensor data are first collected and processed on-device, then analyzed by the embedded AI model, and finally written into the RFID tag for storage and downstream traceability. The complete embedded pipeline, comprising sensor data acquisition, real-time model inference, and RFID tag writing, was successfully deployed on the Arduino Nano 33 BLE MCU. The compiled firmware integrating all three functionalities occupied a moderate portion of the device's available resources. Specifically, the program storage usage accounted for 37% of the total flash memory, while dynamic memory consumption reached 48% of the available RAM as summarized in Table V.

B. RFID Read/Write Performance

The performance of the RFID memory access was evaluated by separately analyzing the writing operation from the MCU

to the RFID tag and the reading operation performed by the portable reader application.

1) MCU-to-Tag Writing Performance: the writing performance was measured by evaluating the time required for the MCU to write the complete set of user memory words to the EM4325 tag over a wired interface. The evaluation was carried out using the example described in Table III. The writing time per byte was measured to be 241.50 μs, demonstrating fast and reliable memory access from the embedded system to the tag.

2) Reader Application Performance: the reading performance was evaluated using a portable UHF RFID reader controlled by a custom Android application. The application interprets the user memory structure described in Table III, transform the retrieved user memory content from HEX to ASCII format, and automatically insert the decoded data into the database. The overall data flow of this process—from reading the tag to decoding and storing the information in the cloud—demonstrated consistent and reliable operation, confirming smooth integration between the RFID reader, decoding module, and backend storage. In addition to functional validation, a preliminary test was conducted to assess the read performance of the RFID system under varying tag orientations. The experiments were carried out in an isolated environment with no nearby metallic objects. When the RFID reader antenna and the tag were positioned face to face (180° alignment), the maximum reliable read range reached approximately 1.5 m at an RF output power of 36 dBm, with a received RSSI of about −42 dBm. When the tag orientation was changed to 45° upward or downward, the tag remained readable at the same distance with similar signal strength. These results indicate that tag orientation had negligible effect on the overall read performance, while the system maintained stable operation within a 1.5 m effective range suitable for handheld harvest applications.

C. Operational Considerations and Cost Assessment

The proposed system was also evaluated in terms of operational efficiency during harvesting. Each cycle begins with sensor data acquisition, followed by tag identification, dual-scan verification, and information writing to the RFID tag. These operations were completed within a few seconds and are therefore negligible in terms of overall cycle time. Considering that a typical harvesting session can last up to six hours [18], [19], the cumulative processing time introduced by the system remains minimal and does not interfere with normal field operations. In the current configuration, sensors collect environmental data every 30 minutes, and inference is executed using both the newly collected data and the previous sample. The resulting classification is then written to the RFID tag. The model operates entirely offline and does not rely on wireless communications, which further enhances energy efficiency and reduces power consumption. These measurements were performed using a Picotest M3510A digital multimeter, while a GW Instek GPS-3303 laboratory DC power supply provided a stable and controlled power source during testing. Power consumption was experimentally evaluated to assess the feasibility of long-term field operation. The system performs one full sensing–inference–RFID writing cycle every 30 minutes.

TABLE VI
BC PERFORMANCE METRICS CONSIDERED IN THE SIMULATED LOCAL ENVIRONMENT

Metric	Result Average
Record Anchoring & Hash Validation	100.0%
Data Integrity Test	Tamper Detected
Storage Growth	2.11 KB (2 blocks)

The active phase consists of approximately 10,000 μs for sensor reading, 700 μs for inference, and 22,218 μs for writing 92 bytes to the RFID tag, resulting in a total active time of about 33 ms per cycle. During this short active window, the MCU draws around 2.5 mA, while in low-power sleep mode—which accounts for the remaining 1799.967 s of the 30-minute interval—the current consumption drops to around 1 mA. Based on these measurements, the average current draw over one full cycle is close to 1 mA, as the MCU remains in sleep mode for more than 99% of the time. Using a compact 50 mAh Li-ion battery, a capacity consistent with the size and weight constraints of handheld harvesting devices, the system achieves around 50 hours of autonomy, corresponding to one or two full harvesting sessions without recharging. Even under conservative derating assumptions to account for environmental variations and voltage regulation losses, the device maintains sufficient energy margin for continuous field operation. These results confirm that the sensing–inference–RFID workflow is fully compatible with lightweight, battery-powered deployment in real harvesting conditions. In terms of cost, the MCU board used in the prototype ranges between 15 and 25 depending on the model, while the sensor costs approximately1–2 and each passive RFID tag costs around 1–2. The RFID reader ranges from 400 to 700, but it is a shared component that can be used across all units during the harvesting process, resulting in a low amortized cost per box. Among these components, only the MCU board represents a relatively high expense, however, it was not specifically designed for this study. The MCU chip itself costs approximately 5, meaning that the higher price mainly comes from the additional peripherals included in the prototyping board (USB interface, voltage regulators, wireless modules, etc.). If a dedicated Printed Circuit Board (PCB) were developed solely for inference and RFID writing—excluding unused capabilities—the cost could be significantly reduced. The current implementation relies on commercially available components for prototyping, while future work will focus on custom, application-specific hardware to further minimize costs and improve suitability for large-scale agri-food deployment.

D. BC-Based Data Integrity

To validate the proposed architecture, a simulated BC environment was implemented and executed locally. The goal was to demonstrate the feasibility and baseline performance of the ledger under controlled conditions, without network latency, distributed consensus, or node synchronization delays. Due to this simulated setting, we focused our evaluation on the metrics that remain meaningful and representative in a local, non-distributed implementation. Specifically, we considered

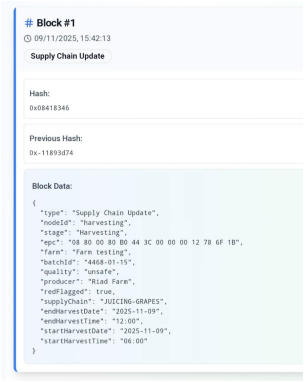


Fig. 9. Screenshot of BC information displayed after scanning the product QR code.

Record Anchoring and Hash Validation, Data Integrity Test, and Storage Growth. These three metrics provide valuable insights into the functionality and robustness of the BC component. Record anchoring and hash validation confirm that data is correctly chained and that any attempt to alter previously recorded information can be detected. The data integrity test further validates the system's ability to identify tampering attempts through hash mismatch checks, while storage growth offers an indication of the overhead introduced by BC anchoring as the number of recorded events increases. In this evaluation, the total storage growth of 2.11 KB corresponded to two recorded blocks, each representing a distinct production stage: the first related to the growing phase and the second to the post-harvesting phase, which is the primary focus of this paper. Metrics such as Transaction Confirmation Time and Throughput (TPS) were deliberately excluded, as they do not provide reliable indicators in a simulated environment. Their values in this context merely reflect local data write speeds rather than actual BC behavior, which in a real-world deployment would depend on consensus algorithms, network conditions, and block propagation times. Including these metrics could therefore lead to misleading interpretations of system performance. The results of the evaluated metrics are summarized in Table VI. The system successfully anchored and validated all submitted records, achieving a 100% success rate. Data integrity checks consistently detected tampering attempts, and storage growth remained minimal, demonstrating the scalability of the proposed approach within the simulated setup. These results indicate that, although the current BC layer operates in a centralized prototype environment, it can emulate core BC functionalities such as record anchoring and hash-based verification. Consequently, the implementation establishes a proof of concept for data immutability and traceability, while full end-to-end transparency and distributed consensus remain objectives for future large-scale deployment.

E. End-to-End Traceability Verification

Fig 9 shows the information retrieved from the RFID tag and visualized through the BC interface after scanning the product's QR code. A single QR code is generated by the platform for each batch and can be attached to the group of harvesting boxes before leaving the farm, ensuring that the whole batch is correctly associated with its traceability record. After scanning, the system retrieves the AI-generated information—previously encoded into the RFID tag and later read by the RFID reader—and displays it in the BC dashboard. The stored record includes the harvest time, farm identity, quality status, and whether the product was red-flagged, confirming both the authenticity of the tag and the proper operation of the end-to-end traceability process.

VI. Discussion and Limitations

A. Threat Mitigation and Security Considerations

In addition to performance and functionality, the proposed RFID–Edge-AI traceability system was also analyzed in terms of potential security threats and corresponding mitigation strategies to ensure data authenticity, integrity, and protection throughout the workflow.

- Tag Cloning or Modification: a common risk in RFID-based systems involves duplicating or altering tag data to falsify product identity. To prevent this, the framework employs a dual-scan mechanism. The first scan verifies that the tag's user memory is empty before any data writing, while the second scan securely links the collected information to that same verified tag, ensuring authenticity and preventing unauthorized tag reuse or cloning. In addition to the dual-scan mechanism, the system can leverage the TID, which is a factory-programmed, read-only serial number embedded within each RFID chip — as a hardware-level safeguard against tag cloning or switching. Because the TID is immutable and unique to each tag, it can be used as a reference counter to verify tag authenticity across multiple scans. During the first registration, both the EPC and TID are stored in the back-end, subsequent scans compare the retrieved TID against the stored record. Any mismatch between the EPC and TID pair immediately indicates potential tag cloning or swapping, thus strengthening the resistance of the system against counterfeit or unauthorized tag replacement.
- Data Tampering: intercepted or modified data during communication between the MCU, RFID reader, and backend could compromise system integrity. This threat is mitigated by anchoring all recorded transactions to the BC layer, which allows any alteration to be detected through hash mismatches and ensures immutable data storage.
- Spoofing or Unauthorized Access: to prevent unauthorized reading or modification of tag data, each RFID tag can be locked with a password. This security measure blocks external RFID readers from overwriting or modifying the tag's user memory, protecting the physical layer of the traceability system.
- Backend Attacks: in the current implementation, the BC operates in a simulated environment that assumes a trusted backend. When deployed with a real BC network, data integrity will be guaranteed through distributed consensus, further improving resilience against backend manipulation or single-point failures.

To systematically evaluate these risks, a threat analysis was conducted following the workflow presented in Fig. 4. Table VII summarizes the primary threats, their preconditions,

TABLE VII
THREAT ANALYSIS AND MITIGATION STRATEGIES IN THE RFID–EDGE-AI PIPELINE

Threat	Preconditions	Likelihood	Impact	Mitigation (linked to Fig. 4 steps)
Tag swap	Physical access to harvest box	Medium	High	Dual-scan verification (Steps 1.a, 2.b) and EPC consistency check in backend (Step 2.d)
Relay attack	Proximity to reader during scan	Low	High	Timestamping and location logging at backend (Step 2.c)
RF shielding	Tag close to metal or moisture	High	Medium	Repeated scans and signal-strength monitoring (Step 2.b)
Sticker removal / reuse	Tag physically detached and reused	Medium	High	Password lock and EPC-to-batch link in backend (Step 2.d)
Password brute-force	Knowledge of tag password scheme	Low	Medium	Strong password policy and limited write attempts (Step 2.a)
EPC collision	Two tags with same EPC	Very Low	Medium	Backend EPC uniqueness check during registration (Step 1.b)

likelihood, potential impact, and the corresponding mitigation strategies, each mapped to the operational steps defined in Fig. 4. As emphasized, passive UHF tags are tamper-evident when combined with the dual-scan and backend anchoring rather than inherently tamper-resistant, providing best-effort authenticity verification across the supply chain. Overall, these mitigation strategies enhance the robustness of the proposed framework by combining physical-level safeguards (RFID authentication and password protection) with data-level defenses (BC-based immutability and controlled writing mechanisms), thereby reinforcing trust and authenticity across all nodes of the system.

B. System Evaluation and Observed Limitations

The results obtained from the prototype implementation demonstrate the feasibility and potential of the proposed RFID-enabled Edge-AI framework for improving traceability, authenticity, and data integrity in agri-food supply chains. By integrating low-cost sensors, on-device intelligence, RFID-based portable storage, and a BC-based audit layer, the system addresses several critical challenges that current solutions still face at the farm level. It enables autonomous environmental monitoring and real-time OTA risk assessment directly in the field, reducing dependence on cloud connectivity and minimizing data transmission overhead. Furthermore, the seamless linkage between edge-generated information and the physical product — achieved through direct RFID writing — enhances data reliability and significantly reduces opportunities for falsification. Another key contribution lies in the system's lightweight design, which lowers the cost barrier for deployment and makes it more suitable for small- and medium-sized producers. The results show that the embedded model maintains high accuracy (>96%) even after quantization and that the on-device inference latency remains below 1 ms, demonstrating the practical viability of real-time decision-making in resource-constrained environments. Importantly, the deployed firmware occupied only 37% of the available flash memory and 48% of the available RAM on the MCU, meaning that less than half of the device's computational resources were consumed. This leaves substantial headroom for deploying larger and more complex AI models or integrating additional preprocessing tasks directly on-device without compromising real-time performance. Despite these promising results, several limitations were identified during the system validation that may influence its performance in real-world scenarios. One limitation is the use of a simulated BC, which, while effective for demonstrating immutability and traceability, does not capture the network latency, consensus overhead, or scalability constraints that would emerge in a distributed deployment. Another limitation concerns the power supply, as the MCU was powered via USB and an external battery during testing — a setup that is not practical in field conditions. Similarly, the current design relies on wired connections between the MCU, Sensor, and RFID tag, which, although stable in laboratory settings, could present challenges in terms of installation complexity and durability in agricultural environments. Additionally, continuous connectivity remains a requirement for certain operations, as the RFID reader still needs internet access to upload data to the backend. This dependency could limit the system's performance in areas with poor or intermittent network coverage. Overall, the system demonstrates strong potential as a secure, low-cost, and autonomous traceability solution, but these limitations highlight important aspects that must be addressed when transitioning from a controlled prototype to real-world deployment. Although the prototype demonstration focused on the harvesting stage, the proposed framework was conceived to function across the entire agri-food supply chain, as illustrated in Fig. 1. Its modular and interoperable design enables adaptation to other stages, including processing lines, where raw materials and machinery parameters can be continuously monitored, and packaging facilities, where product labeling and integrity checks can be integrated into the same RFID-based architecture. This scalability ensures continuity of traceability and authenticity verification across all supply chain stages. RFID is employed throughout harvesting and logistics to ensure secure, machine-readable traceability and physical–digital binding of each product unit, while QR codes are used at the consumer stage to provide universal and low-cost access to verification information. Extending RFID directly to consumers would require each end user to be equipped with an RFID reader, which is not feasible in retail or household environments. From an anti-counterfeiting perspective, QR codes do not constitute the trust anchor of the system, instead, each QR code serves only as an access key to a BC record that is cryptographically bound to the original RFID EPC and TID. Consequently, copying a QR code cannot generate a valid product identity or an authenticated traceability record without a corresponding legitimate RFID-backed BC entry. However, extending the architecture to multiple heterogeneous nodes introduces additional challenges related to interoperability, synchronization, and data consistency, which will be addressed in future developments.

C. Data Protection and Privacy

To ensure secure and responsible data management, the framework restricts the information stored on RFID tags to processed indicators such as OTA class and batch ID.

This design choice ensures that only meaningful, AI-derived information—not raw sensor data—is written to the tag, while complete records are securely maintained in the backend. By recording only essential information, the system effectively overcomes one of the main challenges of IoT architectures—the generation and storage of large volumes of raw data. The example shown in Table III illustrates a complete product record that may originate from the farm; however, in practical deployment, this content can be reduced to only the most relevant fields required for traceability. By transferring essential data instead of full raw records, the system minimizes exposure of sensitive farm information. Access to backend data can be controlled through role-based permissions and field-level encryption, ensuring that only authorized users can view protected fields. The backend can also apply a retention window to automatically remove outdated records, and consumer-facing QR codes display only non-sensitive details such as harvest date and OTA classification. These combined measures preserve transparency while maintaining data privacy across all nodes of the supply chain. To further protect data integrity, versioning control is introduced to prevent rollback attacks: the V field is incremented with each update, and the backend rejects any record whose version is lower than the last accepted value for the same EPC/TID pair. In large-scale deployments, the same RFID tag and MCU can be reused across multiple harvests: each new harvesting cycle generates a new version V and new timestamps (D1, D2), while the BC links all versions to the same EPC/TID pair, thereby preserving a complete and immutable history of successive harvests. At the software level, this versioning mechanism is used to ensure that the QR code and user interfaces display only the data corresponding to the current harvest, while all previous records remain securely stored and auditable in the BC.

VII. Conclusion and Future Perspectives

This study introduced a complete RFID-enabled Edge-AI system designed to enhance traceability, authenticity verification, and data integrity in agri-food supply chains. By combining on-device intelligence with secure RFID storage and BC anchoring, the framework links critical environmental and OTA-risk information directly to the physical product at the moment of harvesting. Although OTA detection was used as the validation scenario, it represents only one application, the modular architecture can be adapted to various sensing or classification tasks across different stages of the supply chain, including processing, storage, packaging, and distribution. Experimental results demonstrate the practicality and robustness of the proposed approach. The Edge-AI module operated efficiently under real embedded constraints, with the MCU remaining active for only 33 ms per measurement cycle, yet still performing sensing, inference, and RFID data preparation. This short active window, together with an average power consumption close to 1 mA, confirms the system's suitability for long-term, battery-powered field deployment. The overall computational footprint was also minimal, leaving ample processing headroom for future extensions or additional sensing tasks. Furthermore, the low per-unit cost makes the solution economically viable for large-scale adoption in agricultural environments. RFID communication was shown to be simple and highly efficient. The first scan writes the EPC and initializes the traceability record, while the second scan retrieves the AI-generated information and uploads it to the backend within a few seconds. This intuitive two-step interaction does not require any specialized technical expertise, as the system autonomously manages data generation, encoding, and retrieval. Additionally, while the MCU writes farm-specific information into the RFID user memory, this part of the workflow is fully customizable and can be adapted to match the specific data requirements of different crops, operations, or traceability regulations. The system also significantly reduces storage requirements by transforming raw sensor streams into compact, high-level information directly on the device, minimizing memory usage on the RFID tag and preventing unnecessary data accumulation. Overall, the prototype validates the feasibility and benefits of a hybrid RFID–Edge-AI–BC architecture for secure, transparent, and low-power traceability in agri-food systems. Future work will focus on integrating a fully distributed BC to assess performance under real consensus mechanisms, designing a dedicated low-power embedded board with an integrated energy solution for autonomous field operation, and implementing a store-and-forward mechanism to maintain data continuity under intermittent reader connectivity.

Acknowledgment

This manuscript reflects only the authors' views and opinions, neither the European Union nor the European Commission can be considered responsible for them.

References

[1] S. Charlebois, N. Latif, I. Ilahi, B. Sarker, J. Music, and J. Vezeau, "Digital traceability in agri-food supply chains: A comparative analysis of OECD member countries," *Foods*, vol. 13, no. 7, p. 1075, Apr. 2024.

[2] S. P. Plakantara and A. Karakitsiou, "Transforming agrifood supply chains with digital technologies: A systematic review of safety and quality risk management," *Oper. Res. Forum*, vol. 6, no. 3, p. 113, Aug. 2025.

[3] *Regulation (EC) no. 178/2002 of 28 January 2002 Laying Down the General Principles and Requirements of Food Law, Establishing the European Food Safety Authority and Laying Down Procedures in Matters of Food Safety*, European Parliament and Council, Brussels, Belgium, Jan. 2002, pp. 1–24.

[4] E. Verna, G. Genta, and M. Galetto, "Enhanced food quality by digital traceability in food processing industry," *Food Eng. Rev.*, vol. 17, no. 2, pp. 359–383, Jun. 2025.

[5] K. Giannakas and A. Yiannaka, "Food fraud: Causes, consequences, and deterrence strategies," *Annu. Rev. Resource Econ.*, vol. 15, no. 1, pp. 85–104, Oct. 2023.

[6] E. Casadei et al., "Emerging trends in olive oil fraud and possible countermeasures," *Food Control*, vol. 124, Jun. 2021, Art. no. 107902.

[7] D. Bose and M. Padmavati, "Honey authentication: A review of the issues and challenges associated with honey adulteration," *Food Bioscience*, vol. 61, Oct. 2024, Art. no. 105004.

[8] M. Mehdizadeh, A. Omidi, S. Morya, and Z. Abideen, "Combating saffron fraud: A systematic review of adulteration practices, detection technologies, recommendations and challenges," *Crit. Rev. Food Sci. Nutrition*, vol. 2025, pp. 1–17, Aug. 2025.

[9] J. O. Pesme, "Tracing and tracking wine bottles: Protecting consumers and producers," *BIO Web Conf.*, vol. 68, Jun. 2023, Art. no. 03028.

[10] D. Skalkos, "Prospects, challenges and sustainability of the agri-food supply chain in the new global economy II," *Sustainability*, vol. 15, no. 16, p. 12558, Aug. 2023.

[11] M. Merenda, C. Porcaro, and D. Iero, "Edge machine learning for AI-enabled IoT devices: A review," *Sensors*, vol. 20, no. 9, p. 2533, Apr. 2020.

[12] R. Colella, A. Arciello, G. Grassi, and M. Merenda, "Memristor-based circuits and architectures enabling next-generation neuromorphic RFID systems," *IEEE J. Radio Freq. Identificat.*, vol. 9, pp. 384–394, 2025.

[13] G. Martino, M. T. Bevacqua, L. Catarinucci, and M. Merenda, "Towards multi-frequency and multi-view localization via UHF-RFID passive tags," in *Proc. IEEE Int. Conf. RFID Technol. Appl. (RFID-TA)*, Dec. 2024, pp. 78–80.
[14] R. E. Venturini, "Technological innovations in agriculture: The application of blockchain and artificial intelligence for grain traceability and protection," *Brazilian J. Develop.*, vol. 11, no. 3, Mar. 2025, Art. no. e78100.
[15] A. Hamdi-Asl, H. Amoozad-Khalili, R. Tavakkoli-Moghaddam, and M. Hajiaghaei-Keshteli, "Toward sustainability in designing an agricultural supply chain network: A case study on palm date," *Scientia Iranica*, vol. 31, no. 18, pp. 1691–1709, 2024.
[16] N. T. N. Trang, T.-T. Nguyen, H. V. Pham, T. T. A. Cao, T. H. T. Thi, and J. Shahreki, "Impacts of collaborative partnership on the performance of cold supply chains of agriculture and foods: Literature review," *Sustainability*, vol. 14, no. 11, p. 6462, May 2022.
[17] Z. Li et al., "Improvement of the sensitivity of lateral flow systems for detecting mycotoxins: Up-to-date strategies and future perspectives," *Comprehensive Rev. Food Sci. Food Saf.*, vol. 23, no. 1, Jan. 2024, Art. no. e13255.
[18] M. R. Sebti, S. Carabetta, M. Russo, and M. Merenda, "Ochratoxin a growth probability estimation in wine production using AI-powered IoT devices," in *Proc. IEEE Conf. AgriFood Electron. (CAFE)*, Sep. 2023, pp. 152–156.
[19] M. R. Sebti, Z. Dakhia, S. Carabetta, R. Di Sanzo, M. Russo, and M. Merenda, "Real-time classification of ochratoxin a contamination in grapes using AI-enhanced IoT," *Sensors*, vol. 25, no. 3, p. 784, Jan. 2025.
[20] D. V. Čepo, M. Pelajić, I. V. Vrček, A. Krivohlavek, I. Žuntar, and M. Karoglan, "Differences in the levels of pesticides, metals, sulphites and ochratoxin a between organically and conventionally produced wines," *Food Chem.*, vol. 246, pp. 394–403, Apr. 2018.
[21] M. Merenda, D. Iero, and F. G. Della Corte, "CMOS RF transmitters with on-chip antenna for passive RFID and IoT nodes," *Electronics*, vol. 8, no. 12, p. 1448, Dec. 2019.
[22] C. Amador, J.-P. Emond, and M. C. D. N. Nunes, "Application of RFID technologies in the temperature mapping of the pineapple supply chain," *Sens. Instrum. Food Quality Saf.*, vol. 3, no. 1, pp. 26–33, Mar. 2009.
[23] F. Gandino, B. Montrucchio, M. Rebaudengo, and E. R. Sanchez, "Analysis of an RFID-based information system for tracking and tracing in an agri-food chain," in *Proc. 1st Annu. RFID Eurasia*, Sep. 2007, pp. 1–6.
[24] A. Corallo, R. Paiano, A. L. Guido, A. Pandurino, M. E. Latino, and M. Menegoli, "Intelligent monitoring Internet of Things based system for agri-food value chain traceability and transparency: A framework proposed," in *Proc. IEEE Workshop Environ., Energy, Struct. Monitor. Syst. (EESMS)*, Jun. 2018, pp. 1–6.
[25] K. Wongpatikaseree, P. Kanka, and A. Ratikan, "Developing smart farm and traceability system for agricultural products using IoT technology," in *Proc. IEEE/ACIS 17th Int. Conf. Comput. Inf. Sci. (ICIS)*, Jun. 2018, pp. 180–184.
[26] M. Merenda, G. Cimino, R. Carotenuto, F. G. D. Corte, and D. Iero, "Edge machine learning techniques applied to RFID for device-free hand gesture recognition," *IEEE J. Radio Freq. Identificat.*, vol. 6, pp. 564–572, 2022, doi: 10.1109/JRFID.2022.3185804.
[27] S. Violino et al., "An artificial intelligence approach for Italian EVOO origin traceability through an open source IoT spectrometer," *Foods*, vol. 9, no. 6, p. 834, Jun. 2020.
[28] N. P. Bhatta and N. Thangadurai, "Utilization of IoT and AI for agriculture applications," *Int. J. Eng. Adv. Technol.*, vol. 8, no. 5, pp. 2731–2735, 2019.
[29] M. T. Gaudio, S. Chakraborty, and S. Curcio, "Agri-food supply-chain traceability: A multi-layered solution," in *Proc. IEEE Int. Conf. Dependable, Autonomic Secure Comput., Int. Conf. Pervasive Intell. Comput., Int. Conf. Cloud Big Data Comput., Int. Conf. Cyber Sci. Technol. Congr. (DASC/PiCom/CBDCom/CyberSciTech)*, Sep. 2022, pp. 1–5.
[30] R. S. Alonso, I. Sittón-Candanedo, Ó. García, J. Prieto, and S. Rodríguez-González, "An intelligent edge-IoT platform for monitoring livestock and crops in a dairy farming scenario," *Ad Hoc Netw.*, vol. 98, Mar. 2020, Art. no. 102047.
[31] K. Fan, W. Jiang, H. Li, and Y. Yang, "Lightweight RFID protocol for medical privacy protection in IoT," *IEEE Trans. Ind. Informat.*, vol. 14, no. 4, pp. 1656–1665, Apr. 2018, doi: 10.1109/TII.2018.2794996.
[32] Arduino.(2025). *Arduino Nano 33 BLE Sense Technical Specifications*. [Online]. Available: https://docs.arduino.cc/hardware/nano-33-ble/#tech-specs
[33] Shenzhen RodinBell Technology.(2025). *Orca 50 Handheld Data Terminal*. [Online]. Available: https://www.rodinbell.com/en/ProductDetail.html?ID=12423
[34] *Regulation (EU) 2022/1370 of 5 August 2022 Amending Regulation (EC) No 1881/2006 As Regards Maximum Levels of Ochratoxin A in Certain Foodstuffs*, European Commission, Brussels, Belgium, 2022.

Mohamed Riad Sebti (Graduate Student Member, IEEE) received the bachelor's degree in computer science with a specialization in computer systems and the master's degree in software engineering and distributed systems from the University of Biskra, Algeria, in 2019 and 2021, respectively. He is currently pursuing the Ph.D. degree with the Mediterranea University of Reggio Calabria (UNIRC), Italy. His research interests include artificial intelligence, embedded systems, and the Internet of Things. He has some publications in the mentioned fields.

Alberto Arciello (Graduate Student Member, IEEE) received the master's degree in electrical and electronics engineering from the Mediterranea University of Reggio Calabria (UNIRC), Italy, in 2024, where he is currently pursuing the Ph.D. degree in electronic engineering. His research activity focuses on neuromorphic computing and emerging memory technologies, examining their applications in secure and energy-efficient embedded systems. He explores hardware security and computational paradigms inspired by biological processes, with a specific emphasis on RFID applications. His research aims to advance the integration of non-volatile memory architectures into next-generation electronic systems, enabling applications ranging from authentication mechanisms to intelligent computing.

Mariateresa Russo received the bachelor's and master's degrees in agriculture from the University of Naples Federico II, Italy, and the Ph.D. degree in food biotechnology from the Mediterranea University of Reggio Calabria (UNIRC) and the University of Bologna, Italy, in 1996. From 1998 to 2000, she was a Post-Doctoral Researcher with the University of Salerno. From 2000 to 2012, she was a Researcher in CHIM/10–food chemistry with the DISTAFA Department, UNIRC. Since 2012, she has been an Associate Professor in CHIM/10–food chemistry with the Department of Agriculture, UNIRC. She has been involved in project management for various complex research projects, all aimed at developing and implementing innovative and sustainable models applied to the main Mediterranean supply chains in the "from farm to fork" perspective. She has served as a principal investigator/scientific responsible for several operational research units (ORs) within each project. Her research interests include food chemistry, authentication, safety, and sensoromics.

Massimo Merenda (Senior Member, IEEE) received the bachelor's, master's, and Ph.D. degrees in electronic engineering from the Mediterranea University of Reggio Calabria (UNIRC), Reggio Calabria, Italy, in 2002, 2005, and 2009, respectively. From 2003 to 2005, he was a fellow with the Institute of Microelectronics and Microsystems of the National Research Council (IMM-CNR), Naples, Italy. From 2011 to 2018, he was a Post-Doctoral Researcher with UNIRC. From 2018 to 2021, he was a Researcher with the DIIES Department, UNIRC, and CNIT. From 2021 to 2022, he was a Senior Scientist with the Cooperative Digital Technologies Competence Unit, Austrian Institute of Technology (AIT), Vienna. Since October 2022, he has been a Senior Researcher with UNIRC, where he has been an Associate Professor since 2025. His research interests include the design of CMOS ICs, silicon sensors, energy harvesting, RFID smart tags and applications, embedded systems, the Internet of Things (IoT), and edge computing for applications of the Internet of Conscious Things and beyond.

Open Access funding provided by 'Univ Mediterranea di Reggio Calabria' within the CRUI CARE Agreement