Survey and Bibliometric Investigation on Communication Technologies for Cold Chain Logistics

Original
Survey and Bibliometric Investigation on Communication Technologies for Cold Chain Logistics / Gandino, F., Ferrero, R.. - In: IEEE ACCESS. - ISSN 2169-3536. - STAMPA. - 14:(2026), pp. 107459-107478. [10.1109/ACCESS.2026.3712272]

Publisher:
Institute of Electrical and Electronics Engineers Inc.

Published
DOI:10.1109/ACCESS.2026.3712272

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 10 April 2026, accepted 1 July 2026, date of publication 10 July 2026, date of current version 20 July 2026.
Digital Object Identifier 10.1109/ACCESS.2026.3712272

SURVEY

Survey and Bibliometric Investigation on Communication Technologies for Cold Chain Logistics

FILIPPO GANDINO, (Member, IEEE), AND RENATO FERRERO, (Senior Member, IEEE)
Dipartimento di Automatica e Informatica, Politecnico di Torino, 100129 Torino, Italy
Corresponding author: Filippo Gandino (filippo.gandino@polito.it)

This work was supported in part by the Project NODES from the MUR—M4C2 1.5 of PNRR under Grant ECS00000036.

ABSTRACT The preservation of perishable goods in cold chain logistics is based on communication technologies that enable continuous monitoring, traceability, and control in production, packaging, storage, transportation, distribution, and retail. This paper presents a comprehensive survey and bibliometric investigation of three key wireless communication technologies: Radio Frequency Identification (RFID), Bluetooth, and ZigBee. Each technology offers substantial benefits, but its practical implementation is shaped by technical and operational challenges, including signal interference, range constraints, environmental harshness, power limitations, and interoperability issues. Through a bibliometric analysis of Scopus and Web of Science indexed literature, this work identifies research trends, sector-specific applications, and disciplinary foci, and outlines emerging technological directions such as multi-protocol Internet of Things integration and long-range communication paradigms. The findings provide insights for researchers, practitioners, and policymakers looking to improve the reliability, efficiency, and transparency of cold chain logistics.

INDEX TERMS Communication technologies, cold chain, cool chain, Bluetooth, RFID, ZigBee.

I. INTRODUCTION

A cold chain is a temperature-controlled supply chain that preserves the quality, safety, and effectiveness of perishable goods throughout handling, storage, and transportation [1]. Its importance is particularly evident in the food and pharmaceutical sectors, where temperature excursions can compromise shelf life, regulatory compliance, and public health outcomes [2], [3]. From production to retail, multiple actors, manufacturers, logistics providers, distributors, and retailers, contribute to maintaining the required thermal conditions [4], [5]. Advanced refrigeration systems, monitoring devices, and optimized packaging solutions help reduce thermal exposure and preserve product integrity [6].

The growing global demand for fresh, high-quality, and temperature-sensitive products has increased the need for reliable, scalable monitoring solutions. Over time, cold chain management has evolved from manual and retrospective temperature checks to integrated wireless systems capable of continuous real-time data acquisition. Among the many technologies explored, Radio Frequency Identification (RFID), Bluetooth, and ZigBee have emerged as the most cited wireless communication solutions for cold chain logistics [7], [8]. RFID enables automated identification and, with sensor-equipped tags, item-level temperature monitoring. Bluetooth supports short-range, energy-efficient communication, and integration with mobile devices. ZigBee provides low-power operation and mesh networking capabilities suited for distributed sensing in warehouses, storage rooms, and transport units.

Although RFID, Bluetooth, and ZigBee are highly valuable, they also face operational limitations. RFID signals can be influenced by liquids, metals, or ice; the limited range of Bluetooth often requires dense deployments; and ZigBee networks can suffer reliability issues in complex or highly dynamic environments. Understanding how the scientific

The associate editor coordinating the review of this manuscript and approving it for publication was Derek Abbott.

literature addresses these advantages and limitations is essential to assess their suitability in cold chain scenarios.

This paper presents a comprehensive survey and bibliometric investigation of RFID, Bluetooth, and ZigBee for cold chain logistics. Using Scopus and Web of Science (WoS) data, the study identifies research trends, disciplinary focus, and sector-specific applications, and synthesizes reported benefits and challenges. The goal is to provide a consolidated view that can support system designers, researchers, and practitioners in selecting or developing effective communication solutions for cold chain monitoring. Beyond the bibliometric perspective, the study also includes a qualitative content analysis of the selected articles. The titles, abstracts, and when available full texts were examined to extract the specific benefits, drawbacks, and technical challenges associated with each technology, as well as the recurring themes and application domains addressed in the literature. This dual quantitative–qualitative approach allows the survey to go beyond a descriptive overview and to highlight comparative patterns, research gaps, and technology-specific insights that are not captured through bibliometric methods alone.

The remainder of the paper is structured as follows. Section II outlines the bibliometric methodology. Section III describes their historical evolution in cold chain applications. Section IV reviews the stages of the cold chain and the role of communication technologies. Sections V and VI examine disciplinary and thematic research trends. Section VII summarizes the benefits attributed to the three technologies, while Section VIII discusses their main limitations. Section IX presents emerging communication paradigms. Section X synthesizes the findings of the bibliometric investigation into decision-oriented insights for practitioners. Finally, Section XI concludes the paper.

II. BIBLIOMETRIC METHODOLOGY

The purpose of the present bibliometric analysis is to provide an overview of the current state and evolution of scientific research. Scopus[1] and WoS[2] were chosen as the primary databases due to their effective indexing capabilities and extensive coverage of scientific articles. Articles were selected based on keywords, including both those provided by authors and those assigned by the analyzed databases [9], [10]. First, to identify the relevant field, the keywords *cold chain* and *cool chain* were used, although the former was overwhelmingly predominant. In addition, communication technologies identified in a previous analysis [8] were added as keywords: *RFID*, *Bluetooth*, and *ZigBee*. These technologies are briefly described later in this section, while the following sections present the findings of the investigation based on both the bibliometric parameters and the content of the articles. The titles, keywords, and abstracts for all articles were reviewed, while the full text was analyzed only when available through open access or institutional subscriptions. Overall, the queries yielded 138 unique articles, and the full text was accessible for 115 of them. When the full text was not accessible, no additional assumptions were made beyond bibliographic metadata and abstract statements. Items requiring full-text evidence (e.g., measured range, battery lifetime, error rates) were coded only when explicitly reported in accessible sections.

Given T as the name of the technology under investigation and C corresponding to the cold chain or the cool chain, the queries executed on Scopus, using its search fields and style, were:

$$(\mathrm{KEY}(C) \wedge \mathrm{KEY}(T)) \tag{1}$$

The queries executed in WoS turned out to be more complex since this database uses two distinct fields for author-assigned keywords and database-assigned keywords. The resulting queries were as follows:

$$\begin{aligned} &T(\text{Author Keywords}) \wedge C(\text{Author Keywords}) \vee \\ &T(\text{Author Keywords}) \wedge C(\text{Keyword Plus}^{®}) \vee \\ &T(\text{Keyword Plus}^{®}) \wedge C(\text{Author Keywords}) \vee \\ &T(\text{Keyword Plus}^{®}) \wedge C(\text{Keyword Plus}^{®}). \end{aligned} \tag{2}$$

The bibliometric dataset also enabled the execution of keyword co-occurrence and co-authorship analyses. These network-based analyses, conducted using the VOSviewer software,[3] complement traditional bibliometric indicators by revealing latent structures in the literature, such as thematic clusters, collaborative patterns, and emerging research communities. As a result, they provide a deeper and more interpretable view of how research on communication technologies for the cold chain is organized and evolves over time.

To construct the dataset for these analyses, Scopus and WoS records were merged into a unified corpus. Because many WoS publications also appear in Scopus, the aggregation was designed to avoid over-weighting duplicated entries. Scopus was therefore used as the primary source for keyword extraction, including both author-supplied keywords and Scopus-indexed terms. From WoS, only documents not indexed in Scopus were added, and for these records both author and database assigned keywords were considered. In building the keyword network, the exact keywords used to formulate the database queries (e.g., "RFID", "Bluetooth", "ZigBee", "cold chain", "cool chain") were deliberately excluded, to prevent search terms from dominating the co-occurrence structure and to ensure that the resulting network reflects thematic relationships emerging from the literature rather than artifacts of the retrieval process. This strategy ensures complete coverage of the corpus while avoiding artificial inflation of keyword frequencies or co-occurrence strengths.

The resulting consolidated dataset enables meaningful network analyses: keyword co-occurrence mapping identifies

[1] https://www.scopus.com
[2] https://www.webofscience.com
[3] https://www.vosviewer.com/

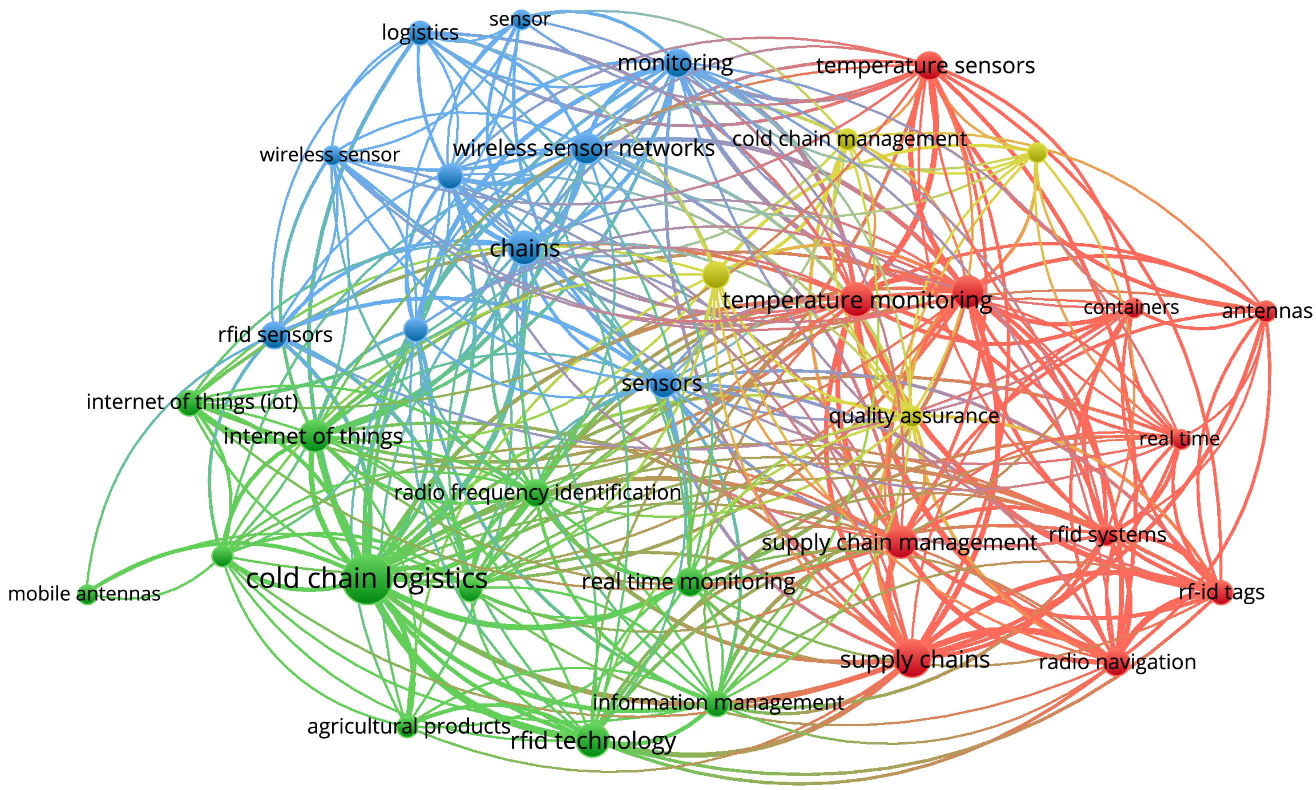

FIGURE 1. Keyword co-occurrence network for publications containing both "RFID" and "cold chain" (or "cool chain") in the merged Scopus–WoS dataset. Only keywords appearing in at least five articles were included.

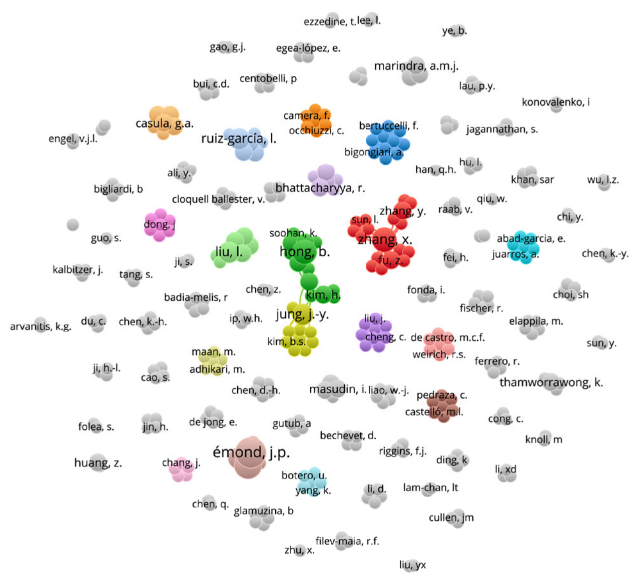

FIGURE 2. Co-authorship network derived from the merged Scopus–WoS dataset for publications containing both "RFID" and "cold chain" (or "cool chain"). No minimum publication threshold was applied.

conceptual clusters and shows how topics relate to one another, while co-authorship networks highlight collaborative dynamics across institutions and regions. These insights cannot be obtained from publication counts alone and play a crucial role in characterizing the structure, maturity, and fragmentation of the research landscape.

A. QUALITATIVE CONTENT ANALYSIS AND REPRODUCIBILITY

In addition to the bibliometric indicators, a qualitative content analysis was conducted to extract (i) reported benefits, (ii) reported limitations/challenges, (iii) main application domains, and (iv) research topics addressed by each study. A structured coding scheme (codebook) was adopted and applied at paper level. Coding focused on benefits, limitations, and application domains, using titles/abstracts/keywords for all papers, and full texts when accessible. Multiple labels per paper were allowed; ambiguous claims were not coded. This qualitative coding complements the bibliometric indicators by providing an interpretative layer that supports the comparative analyses developed in the subsequent sections.

Unit of analysis. Each publication represents one unit. Coding was performed primarily on titles, abstracts, and keywords for all papers, while the full text was used when accessible.

Codebook and classification rules. Categories were defined a priori based on the survey objectives (technology comparison, application context, and deployment constraints). A paper was assigned to a category only when an explicit statement (or a clearly implied claim supported by results) was present in the abstract or full text. Multiple labels were allowed (e.g., a paper could report both ''low cost'' and ''robustness'' as benefits). Ambiguous claims (e.g., generic statements without evidence) were not coded. Coding was performed by the authors using the shared codebook. Unclear cases were discussed until consensus was reached, and items were coded only when supported by explicit statements.

Treatment of partially accessible papers. For papers without accessible full text, classification relied exclusively on title/abstract/keywords. Full-text-only evidence (e.g., detailed quantitative performance results) was not inferred. To mitigate bias, the qualitative synthesis focuses on recurring claims observed across multiple papers and explicitly reports the number of occurrences for each coded item (see Section VII and Section VIII).

Reproducibility. The complete codebook (category definitions and inclusion rules) used for qualitative analysis is provided in specific tables in each section to enable replication and future extensions.

B. RFID

RFID is an automatic identification technology that uses electromagnetic fields to detect and track objects equipped with RFID tags. An RFID system typically consists of tags (transponders), readers (interrogators), and a back-end system for data processing. RFID tags can be passive (powered by the reader's signal), active (with their own battery), or semi-passive (battery-assisted, but only activated by the reader).

RFID operates in several frequency bands, namely Low Frequency (LF), from 125 to 134 kHz, High Frequency (HF), at 13.56 MHz, and Ultra-High Frequency (UHF), from 860 to 960 MHz. UHF RFID provides long read ranges (up to 12 meters) and fast data rates, making it the most suitable for inventory tracking and supply chain management.

RFID communications are regulated by protocols that handle collision, data encoding, and security and ensure interoperability between tags and readers from different manufacturers. The most prominent protocols are the ISO/IEC 18000 series, which specifies the air interface for different frequency ranges. For example, ISO/IEC 18000-2 covers LF, ISO/IEC 18000-3 covers HF, and ISO/IEC 18000-6C (also known as EPCglobal Gen2) concerns UHF.

Figure 1 provides additional insight into the role of RFID within the broader research landscape by showing the keyword co-occurrence network derived from the merged Scopus–WoS dataset. Only keywords appearing in at least five publications were included, so that the resulting structure highlights consolidated thematic patterns rather than sporadic terms.

Although the keyword ''RFID'' is excluded by this analysis, RFID-related keywords (such as ''radio frequency identification'', ''rfid sensors'', and ''rf-id tags'') occupy a central position on the map and exhibit strong connections with clusters linked to cold chain logistics, supply chain management, and temperature monitoring. This confirms that RFID is not only employed for automatic identification, but is also tightly integrated with broader themes such as real-time monitoring, information management, and quality assurance. The proximity of RFID terms to nodes such as ''wireless sensor networks'', ''containers'', and ''agricultural products'' further indicates the widespread applicability of RFID in multiple stages and cold chain sectors. In general, the structure of the network highlights the centrality of RFID in cold chain communication research and its intersection with both the technological and application-driven domains.

Figure 2 shows the co-authorship network generated from the same RFID–cold chain dataset used for the keyword analysis. In this case, no minimum publication threshold was imposed, so all authors appearing in the selected corpus are represented in the map. The resulting structure highlights several well-defined collaborative groups, each corresponding to clusters of researchers who frequently co-author studies on RFID applications in cold chain logistics. Larger nodes denote authors with a higher number of publications or co-authorship links within the dataset, while the spatial proximity of nodes reflects the intensity of collaboration among researchers or research teams.

The presence of multiple distinct clusters suggests that RFID research in the cold chain domain is distributed across independent research communities, often geographically or institutionally concentrated. Some clusters are tightly interconnected, indicating stable collaborative networks working on closely related topics such as temperature monitoring, wireless sensor integration, or RFID-based traceability, whereas others appear more dispersed, reflecting occasional or cross-domain collaborations. Overall, the co-authorship network complements the keyword analysis by revealing the human and institutional structure underpinning the development of RFID solutions for cold chain monitoring.

C. ZigBee

ZigBee is a wireless communication technology based on the IEEE 802.15.4 standard, designed for low-power, low-data-rate, and short-range applications. ZigBee is used primarily in wireless personal area networks (WPANs), but it is also well-suited for industrial control applications and sensor networks. ZigBee operates mainly in the following frequency bands: 2.4 GHz (16 channels with a maximum data rate of 250 kbps), 868 MHz (single channel with a data rate of 20 kbps), and 915 MHz (10 channels with a data rate of 40 kbps).

The ZigBee protocol stack is structured into several layers: the physical layer, the media access control layer, the network layer, and the application layer. The protocol defines mechanisms for device addressing, network formation, security (using AES-128 encryption) and mesh networking, which allows devices to relay data through intermediate nodes for greater range and reliability.

ZigBee devices are categorized into three types: ZigBee Coordinator (central controller), ZigBee Router (extends network coverage), and ZigBee End Device (sensors or

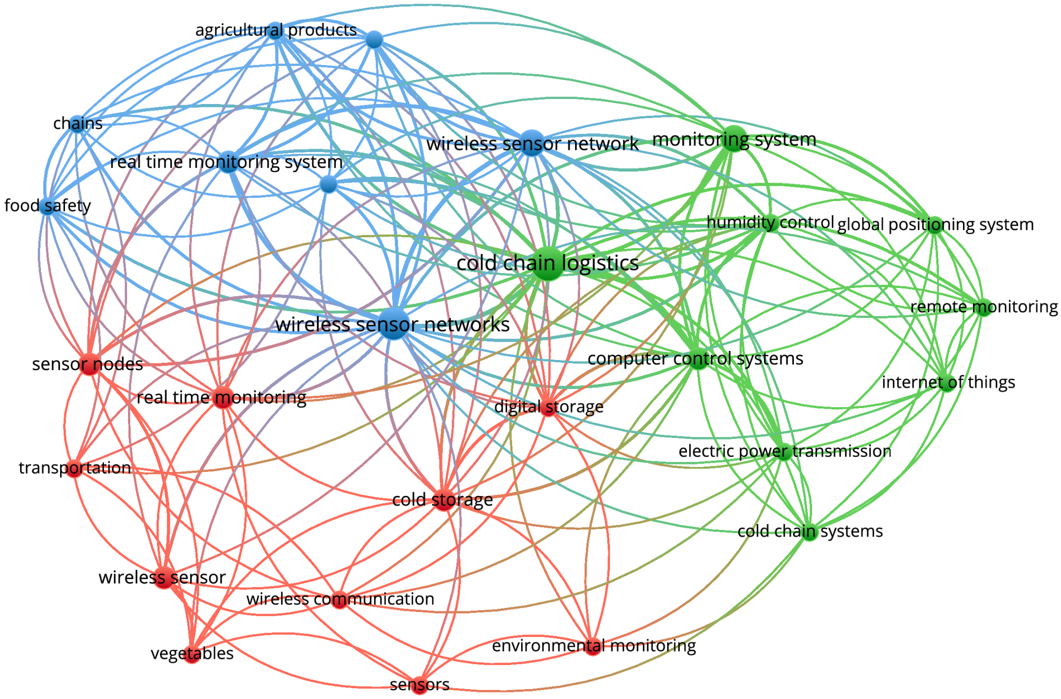

FIGURE 3. Keyword co-occurrence network for publications containing both "ZigBee" and "cold chain" (or "cool chain") in the merged Scopus–WoS dataset. Only keywords appearing in at least two articles were included.

actuators with limited functions). The protocol supports star, tree, and mesh topologies, enabling flexible and scalable network architectures. The low power consumption of ZigBee makes it ideal for battery-operated devices that need to run for extended periods without maintenance.

Figure 3 shows the keyword co-occurrence network obtained from the merged Scopus–WoS dataset restricted to publications containing both "ZigBee" and "cold chain" (or "cool chain"). Given the smaller number of ZigBee-related papers compared to RFID, a lower inclusion threshold was adopted: only keywords that appeared in at least two publications were retained. This ensures sufficient density in the network while still reflecting recurrent concepts within the available literature.

The resulting map reveals several interconnected thematic clusters. ZigBee is closely associated with terms related to wireless sensor networks (e.g., "wireless sensor network", "sensor nodes"), real-time monitoring and environmental or cold storage monitoring. The strong co-occurrence links connecting ZigBee-related terms with "cold chain logistics", "monitoring system", and "remote monitoring" highlight the central role of ZigBee in distributed sensing applications, particularly where multi-hop or scalable network topologies are advantageous. Other clusters emphasize links with agricultural products, food safety, and environmental monitoring, reflecting the use of ZigBee-based sensor networks in both warehouse storage and perishable goods management.

In contrast to RFID, a co-authorship network is not reported for ZigBee, because the number of contributing authors is limited and the resulting graph is highly fragmented.

D. BLUETOOTH

Bluetooth is a wireless communication technology designed for short-range data exchange between devices. It operates in the 2.4 GHz ISM (Industrial, Scientific and Medical) frequency band, using frequency-hopping spread spectrum to minimize interference and enhance communication reliability. The standard range for Bluetooth is typically up to 10 meters (Class 2 devices), but can reach up to 100 meters for Class 1 devices.

Bluetooth specifications are maintained by the Bluetooth Special Interest Group (SIG). Earlier IEEE 802.15.1 standardization efforts historically described Bluetooth-based WPANs, but the IEEE 802.15.1 standard is now withdrawn. The most widely used protocol versions are Bluetooth Classic (BR/EDR) for continuous data streaming and Bluetooth Low Energy (BLE or Bluetooth Smart) for applications requiring low power consumption and intermittent data exchange.

Bluetooth networks use a central-peripheral architecture (referred to as "central" and "peripheral" in BLE), where one device acts as the central and controls the communication with one or more peripheral devices. Bluetooth supports both point-to-point and multipoint (piconet and scatternet)

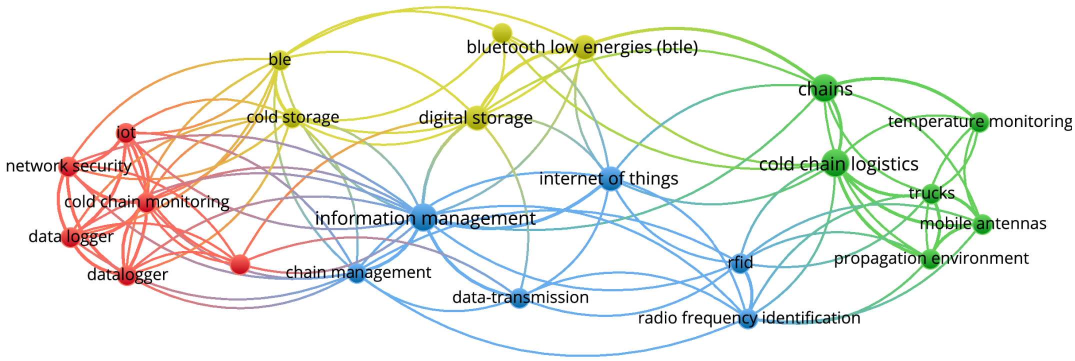

FIGURE 4. **Keyword co-occurrence network for publications containing both "Bluetooth" and "cold chain" (or "cool chain") in the merged Scopus–WoS dataset. Only keywords appearing in at least two articles were included.**

network topologies. Security mechanisms such as pairing, authentication, and encryption are integrated into the protocol to ensure data confidentiality and integrity.

Figure 4 shows the keyword co-occurrence network obtained from the merged Scopus–WoS dataset restricted to publications containing both "Bluetooth" and "cold chain" (or "cool chain"). As for the ZigBee analysis, the number of available publications in this subset is relatively small, so a threshold of at least two occurrences was adopted for keyword inclusion.

The resulting network reveals several thematic clusters that reflect the typical roles of Bluetooth technologies in cold chain monitoring. Keywords related to BLE, cold storage, digital storage, and information management form a tightly connected group, indicating the emphasis on short-range sensing, data logging, and local monitoring infrastructures. Another prominent cluster links Bluetooth to the Internet of Things (IoT), network security, and data-transmission concepts, highlighting the integration of BLE-based devices into broader IoT architectures for distributed monitoring.

Additional connections to terms such as "temperature monitoring", "cold chain logistics", and "mobile antennas" show that Bluetooth is increasingly used in real-time monitoring applications and in mobile or vehicle-mounted scenarios, often complementing other communication technologies. In general, the network structure confirms that Bluetooth plays a bridge role between local sensing and IoT-enabled data management within cold chain systems.

Due to the limited number of authors contributing to this subset of the literature and the resulting fragmentation of the co-authorship graph, an author network is not included for the Bluetooth analysis.

III. EVOLUTION OF COMMUNICATION TECHNOLOGIES IN THE COLD CHAIN

Communication technologies in cold chain logistics have progressively evolved to meet the growing requirements of identification, monitoring, traceability, and rapid response. Early systems relied on manual checks and simple electronic data loggers that offered only retrospective temperature information, making it difficult to detect or prevent thermal deviations during transport and storage [11].

A first major technological step was the adoption of RFID systems in the late 1990s and early 2000s. RFID enabled automated, non-line-of-sight identification of pallets and packages, and temperature detection tags (smart tags) introduced item-level thermal monitoring [12]. These systems significantly improved inventory management and traceability, although their operational use was often limited to checkpoints and was limited by infrastructure and cost considerations [13].

By the mid-2000s, Wireless Sensor Networks (WSNs) based on ZigBee technology addressed some of the limitations of RFID by providing continuous temperature and humidity monitoring. Real-time alerts reduce spoilage risks and improve responsiveness in warehouses and transport operations [14], [15]. The mesh network capability of ZigBee improved coverage in complex environments, although the installation and maintenance of the router nodes remained challenging [16].

Around 2010, BLE and IoT platforms introduced further advances. BLE allowed cost-effective integration with mobile devices, allowing rapid access to temperature data during loading, unloading, or retail operations [17]. The IoT architectures consolidated heterogeneous sensors, gateways, and cloud services, enabling continuous data flow throughout the production, storage, transportation, and distribution stages [18]. This convergence supports predictive analytics, automated alerts, and comprehensive traceability, changing cold chain management from reactive verification to proactive quality assurance [19].

Figure 5 illustrates the research interest in RFID, ZigBee, and Bluetooth up to 2024. RFID, due to its earlier adoption, shows sustained attention over time. ZigBee gained prominence in the early 2010s with the expansion of WSN applications, and after a break, it has regained interest in recent years. BLE attracted growing attention after 2013, reflecting the rise of mobile-centric monitoring solutions.

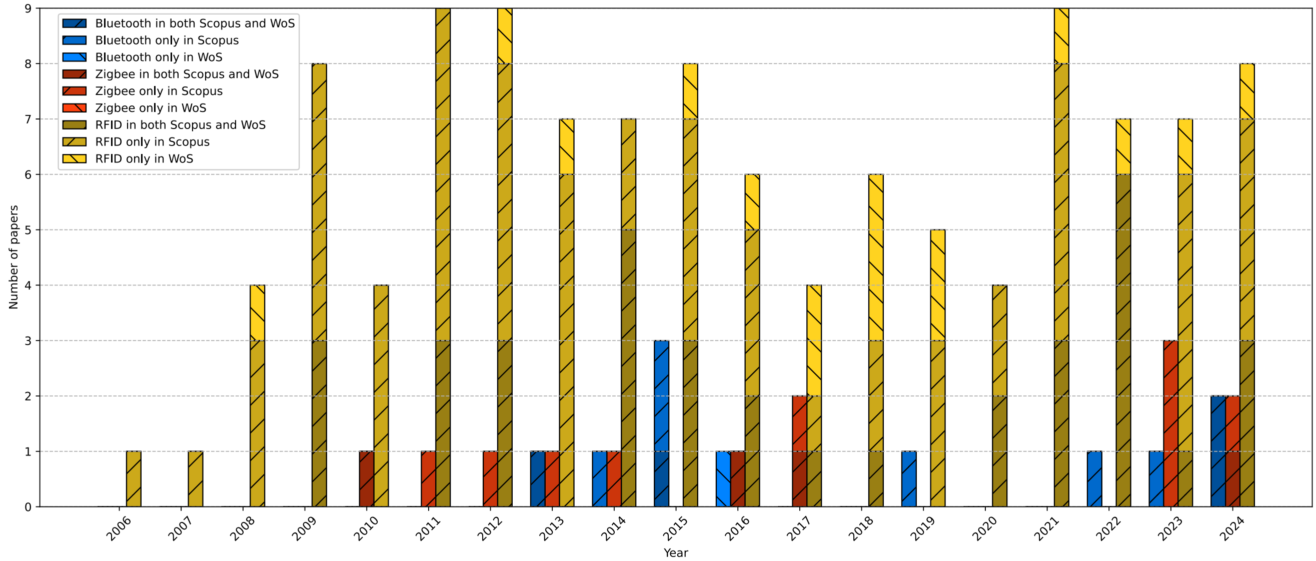

FIGURE 5. Number of articles indexed by Scopus and WoS per year mentioning one between "cold chain" or "cool chain" and one of the technologies: RFID, ZigBee or Bluetooth.

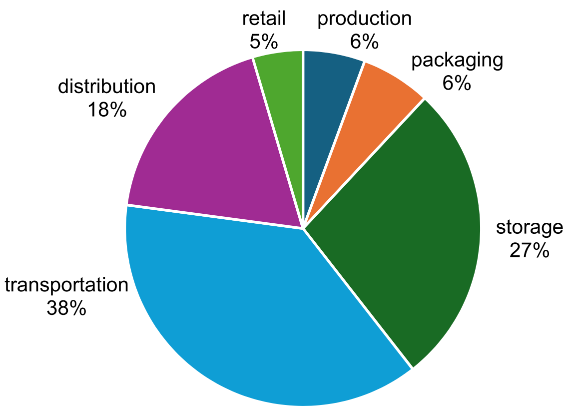

FIGURE 6. Classification of the contribution of articles indexed by Scopus and WoS throughout the cold chain stages.

IV. COLD CHAIN STAGES

Cold chain logistics can be decomposed into a sequence of stages (i.e., production, packaging, storage, transportation, distribution, and retail), in which products must be handled under controlled thermal conditions. Communication technologies support these activities by enabling environmental monitoring, traceability, and rapid detection of deviations. Figure 6 shows the contribution of the analyzed literature to each stage. Since many studies span multiple phases, a single paper may contribute to more than one category. The following subsections discuss typical operations carried out at each stage and the role played by wireless communication technologies.

A. PRODUCTION (MANUFACTURING AND HARVESTING)

The cold chain begins at the production site, where temperature stabilization is essential to ensure quality and safety. Fresh produce is precooled shortly after harvest to remove field heat, while fish or meat are chilled or frozen soon after processing to inhibit microbial growth. Pharmaceuticals such as vaccines are immediately stored in controlled facilities to preserve their potency [18]. Communication technologies support this stage by enabling environmental monitoring (temperature, humidity, gases) [20], integrating automatic product identification into monitoring systems [21], and supporting quality control checks before shipment [22].

B. PACKAGING

Packaging involves both the physical configuration of the product and the incorporation of materials or devices that help maintain temperature during transport. Perishable foods can be packed with gel ice packs or dry ice in insulated containers, while vaccines and biotech products use thermal packaging with phase-change materials. Although the literature focuses less on packaging innovations compared to other stages, communication technologies play an important role by enabling real-time data collection from embedded sensors and ensuring traceability and positioning [23], [24].

C. STORAGE (COLD WAREHOUSING)

Storage occurs at various points in the supply chain, including cold warehouses in manufacturing sites, refrigerated distribution centers, or storage rooms in logistics centers. The maintenance of stable temperatures for extended periods makes this stage one of the most studied. Communication technologies are used to continuously monitor environmental conditions [25] and to support inventory management tasks such as product identification and location tracking [26].

D. TRANSPORTATION (REFRIGERATED TRANSIT)

Transportation is often the most vulnerable link in the cold chain, as products are exposed to external heat loads, door openings, traffic delays, and limited operator oversight. Monitoring technologies aim to provide real-time visibility and rapid response capabilities. Temperature alerts can be sent to drivers or fleet managers whenever conditions exceed safe thresholds [27]. Location tracking improves traceability [28] and, combined with route optimization [29], [30], supports timely interventions, such as redirecting to the nearest cold storage facility in case of a malfunction [31]. These capabilities improve both product integrity and logistics planning.

E. DISTRIBUTION (CROSS-DOCKING AND INTERMEDIATE HANDLING)

Distribution nodes act as intermediaries between long-haul transportation and retail or final delivery. Their communication needs combine those of storage and transportation. Technologies that integrate identification and temperature monitoring make it possible to retrieve the full thermal history of incoming products, update inventory records, and maintain traceability between transfer points [32]. Cloud platforms that aggregate data from production, transport, and storage allow stakeholders to access up-to-date information and make informed decisions at distribution hubs [33].

F. RETAIL (ENDPOINT STORAGE AND DISPLAY)

Retail settings such as supermarkets, pharmacies, and hospitals store products on site until they are sold or administered. Communication technologies ensure safety, quality assurance, and final traceability [34]. Continuous monitoring helps detect equipment malfunctions or temperature deviations, while integration with inventory systems closes the traceability loop by linking storage data with point-of-sale information [35].

V. DISCIPLINARY FOCUS IN COLD CHAIN COMMUNICATION TECHNOLOGIES

To better understand how communication technologies are studied and applied within cold chain logistics, the retrieved articles were categorized by their scientific field. Figure 7 shows the normalized frequency with which each sector addresses Bluetooth, ZigBee, and RFID. Since Scopus and WoS use different classification schemes, several fields were harmonized: Scopus categories such as "Economics, Econometrics and Finance" and "Business, Management and Accounting" were grouped under the WoS "Business & Economics," while "Automation & Control Systems," "Education & Educational Research," "Food Science & Technology," and "Telecommunications" were aligned with the corresponding Scopus fields.

The results highlight clear disciplinary patterns:

- **Engineering** is the dominant field in all technologies, reflecting the predominantly technical challenges associated with cold chain monitoring, communication reliability, and system integration [36].
- **Computer Science** is particularly prominent for RFID, reflecting its strong links to data management, middleware, and interoperability research [37]. However, Bluetooth and ZigBee also have significant representation, consistent with their extensive use in wireless sensor network studies.
- **Mathematics** and **Decision Sciences** appear more frequently in Bluetooth and ZigBee studies, likely linked to logistics optimization, algorithmic resource allocation, and simulation-based analyses.
- **Physics, Chemistry, and Biochemistry** show a higher representation in ZigBee research, reflecting its use in monitoring environmental or biochemical conditions in scientific experiments and storage trials.
- **Economics** appears occasionally, with ZigBee and RFID contributing studies focused on supply chain management, regulatory aspects, or economic efficiency.
- **Agricultural and Biological Sciences** are well represented for ZigBee and RFID, as these technologies are often applied in food logistics, agricultural produce monitoring, and biological sample management [38].
- **Medicine** appears more frequently in RFID-related work, consistent with its adoption in pharmaceutical logistics and hospital inventory systems.

In general, the disciplinary distribution reflects both the maturity of RFID in various industrial domains and the technical nature of ZigBee and Bluetooth-based deployments. The presence of ZigBee in the natural sciences confirms its role in sensing-driven applications.

VI. RESEARCH FOCUS

Figure 8 shows the distribution of the main research topics addressed by studies focusing on Bluetooth, ZigBee, and RFID in cold chain applications. Frequencies are normalized for each technology by dividing the count of each topic by the maximum observed for that technology, allowing for comparison of relative prominence rather than absolute publication numbers.

Several patterns emerge:

- **Framework development** is the most frequently addressed topic across all technologies [39], [40], [41], reflecting the common need to integrate sensors, communication modules, and cloud platforms into coherent architectures.
- **Antenna design and optimization** are prominent for Bluetooth [42] and RFID [43], due to the importance of ensuring reliable communication in dense and harsh environments. For Bluetooth, antenna-related work is especially visible, likely due to its interaction with packaging materials and container structures.
- **Sector-specific applications** (e.g., food, pharmaceuticals, or vaccines) appear with moderate frequency in all technologies [44], [45], [46], demonstrating the emphasis on adapting solutions to distinct operational needs.

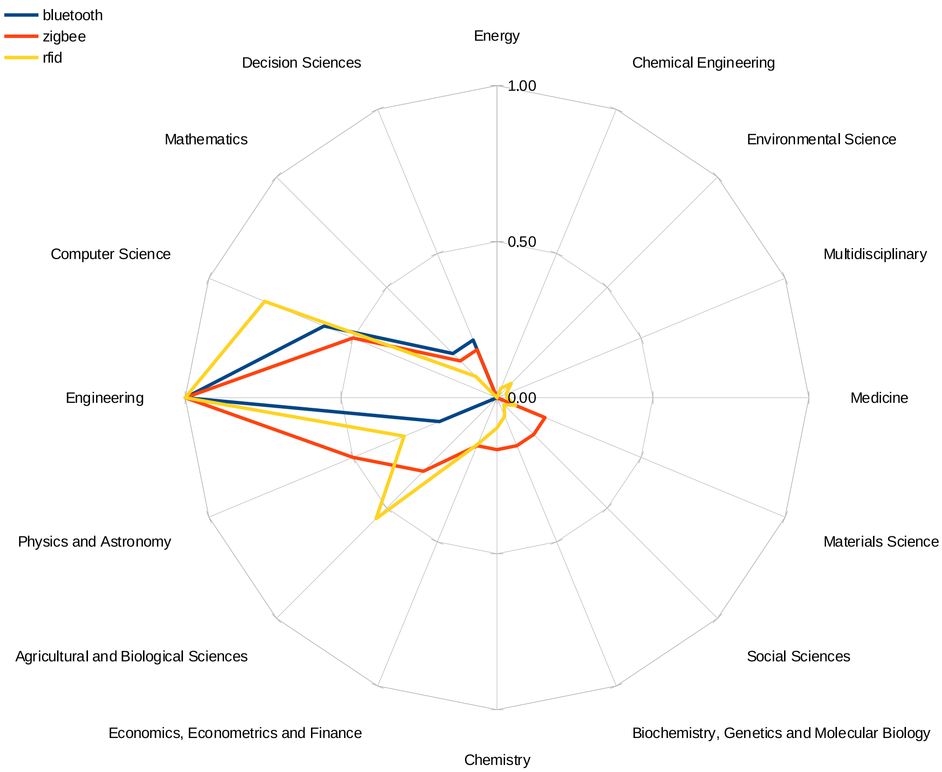

FIGURE 7. Relative frequency of scientific fields represented in publications on Bluetooth, ZigBee, and RFID technologies for the cold chain, based on a Scopus and WoS literature survey. The values are normalized for each technology to the sector with the highest representation (Bluetooth=5, ZigBee=6, and RFID=31).

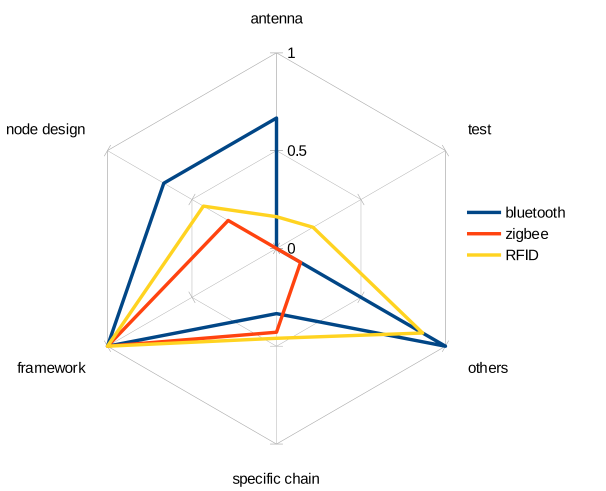

FIGURE 8. Frequency of major research topics for Bluetooth, ZigBee, and RFID in the cold chain literature, based on Scopus and WoS review. The values are normalized for each technology to the sector with the highest representation (Bluetooth=3, ZigBee=7, and RFID=37).

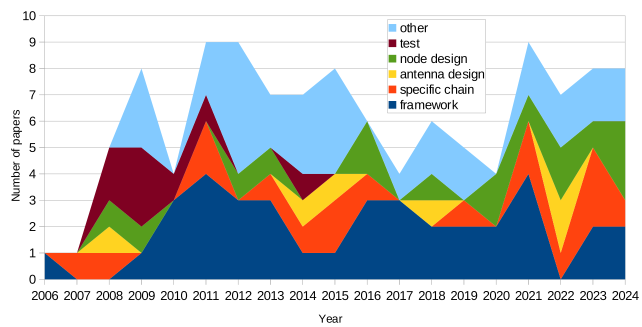

FIGURE 9. Evolution of the frequency of major research topics for RFID in the cold chain literature, based on Scopus and WoS review.

- **Node design** is common to all technologies, but occurs more frequently for Bluetooth [47], then RFID [36], [48] and finally ZigBee [25], reflecting the development of custom sensor nodes, prototypes, or experimental deployments.
- **Testing** is peculiar only for RFID, where it represents a consistent topic.
- The **others** category includes emerging or niche topics such as smart devices [49], risk management [50], vehicle routing [51], and traceability analyses [52],

TABLE 1. Qualitative codebook used to classify the main *research topics* addressed by each paper.

Topic category	Inclusion rule (a paper is coded if it...)
Framework development	Proposes or formalizes an end-to-end architecture/framework integrating sensing, communication, and data management (e.g., gateway, cloud platform, middleware, data pipeline) for cold chain monitoring/traceability.
Antenna design	Designs, models, prototypes, or optimizes antennas/RF front-end aspects (e.g., tag/reader antennas, matching networks, placement/orientation, packaging effects, propagation/attenuation studies) with the explicit goal of improving link quality or readability in cold-chain conditions.
Sector-specific applications	Targets a specific vertical or product class (e.g., food, meat/fish, produce, dairy, pharmaceuticals, vaccines, blood/biological samples) and discusses requirements, constraints, or validation tailored to that sector rather than generic cold-chain monitoring.
Node design	Develops or customizes a sensing/communication node (hardware and/or embedded firmware), including sensor integration, energy management, packaging/enclosure design, or device-level prototyping beyond off-the-shelf deployment.
Testing	Reports experimental validation or trials (lab tests, pilot deployments, field trials) with measurable outcomes (e.g., read rate, range, packet loss, temperature accuracy, latency) in cold-chain relevant settings.
Others (emerging/niche)	Addresses topics not covered above, such as smart devices, risk management, vehicle routing/optimization, traceability analytics, blockchain integration, security protocols, or other specialized methods not central to the main five categories.

which are more represented in RFID research due to its broader range of applications.

In general, the mapping of the research focuses reflects both the technological characteristics and maturity levels of the three solutions: Bluetooth research emphasizes communication reliability and integration, ZigBee focuses on distributed sensing and network architectures, and RFID spans hardware design, system-level considerations, and diverse application domains. Figure 9 provides more information on RFID, the technology associated with the largest number of papers. This figure illustrates the evolution of the topics addressed over the years. It can be observed that most themes are distributed across the entire time span, with the exception of articles focused on testing, a topic that initially attracted considerable interest but gradually declined. In contrast, studies on antennas, which account for a comparable number of papers, are instead spread across the entire period.

Therefore, the research themes shown in Fig. 8 are the result not only of the publication frequencies but also of a qualitative assessment of how each study positions the technology within the cold chain. This combined approach enables a more nuanced comparison between technologies, highlighting how research priorities align, or misalign, with their practical challenges and deployment contexts. The codebook applied to classify the papers is reported in Table 1.

VII. BENEFITS OF COMMUNICATION TECHNOLOGIES

Figure 10 summarizes the main benefits associated with RFID, Bluetooth, and ZigBee in cold chain logistics. Each technology is linked to distinct strengths that reflect both its design characteristics and its typical deployment scenarios. The benefits summarized in the figure originate from a qualitative synthesis of the claims and findings reported in the analyzed articles, rather than solely from keyword frequencies. This enables a technology-specific evaluation grounded in a detailed reading of the literature. The codebook applied to classify the papers is reported in Table 2.

RFID is frequently recognized for its low cost [48], especially in the case of passive tags, which are inexpensive and do not require onboard power [53], [54]. This enables widespread item-level deployment at competitive cost compared to active sensors [55]. RFID tags are also appreciated for their robustness in cold environments [34], ease of use [52], flexibility [56], and long service life [57]. Additional benefits include printability [58], increased memory capacity [59], and physical flexibility that allows roll-up or curved-surface applications [60].

Bluetooth-based solutions, particularly BLE, are praised for their integration with smartphones [17], [61] and energy efficiency [40]. Compatibility with consumer devices simplifies deployment and data retrieval, allowing personnel to access temperature logs or real-time alerts without dedicated readers. The low-power design of the BLE enables long battery life, an essential feature for monitoring shipments over long periods. Additional benefits include high antenna sensitivity [42], short communication latency [17], the ability to wake up devices on demand [17], and operation without centralized coordination [45].

ZigBee is highly valued for its mesh networking capabilities [62], which allow nodes to relay data and self-organize into scalable networks that can cover large storage facilities or long-distance transport units. Designed for low-power wireless sensor networks [63], [64], ZigBee is often associated with benefits such as power efficiency [65], reliability [66], and extended communication range compared to other short-range standards [62]. The high data transfer speed in local WSNs has also been reported as an advantage for certain deployments [63].

In general, the benefits attributed to the three technologies overlap only partially. Bluetooth and RFID offer largely distinct advantages, while Bluetooth and ZigBee share an emphasis on energy efficiency. RFID and ZigBee offer both low-cost or high-throughput communication advantages depending on the deployment context.

VIII. CHALLENGES AND LIMITATIONS IN TECHNOLOGY DEPLOYMENT

Although wireless communication technologies offer valuable capabilities for cold chain logistics, several challenges

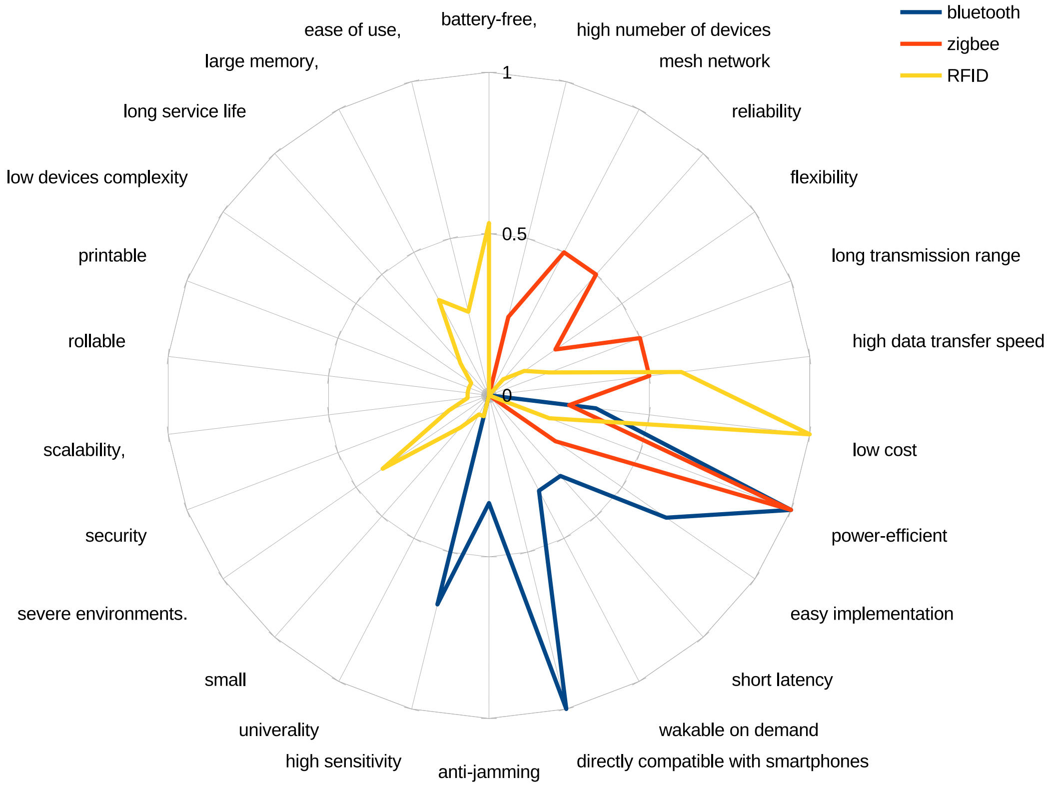

FIGURE 10. Distribution of benefits attributed to RFID, Bluetooth and ZigBee technologies in cold chain logistics, as identified by a systematic review of the literature on Scopus and WoS. The values are normalized for each technology to the sector with the highest representation (Bluetooth=3, ZigBee=4, and RFID=15).

and limitations affect their reliability, scalability, and integration. Figure 11 highlights the most frequently cited issues related to RFID, but similar concerns, in different forms, also apply to Bluetooth and ZigBee. The following subsections summarize the main technical and operational constraints discussed in the literature.

The challenges were identified through qualitative coding using the categories in Table 3. The classification captures the recurring types of technical, operational, and organizational limitations discussed in the literature. For RFID, the larger corpus allows reporting occurrence counts. For Bluetooth and ZigBee, given the smaller number of studies that address limitations, the analysis is more anecdotal, without strong statistical relevance. Therefore, challenges are qualitatively discussed and grouped according to the same classification scheme, without reporting frequencies.

A. RFID ISSUES

RFID technology has been extensively studied in the cold chain, yet several obstacles still limit its adoption. The most frequently cited issue is *interference* [67] (14 times), particularly from metal, moisture, and ice, which can degrade signal quality and reduce readability. The *High implementation cost* [68] (7 times) also remains a concern, especially when estimating the deployment and integration of the infrastructure, although the operational tag costs may be low.

A further limitation is the *lack of global standardization* [69] (6 times), which complicates the interoperability between supply chain actors. Other issues include *data security* [57] (5 times), *memory constraints* [56] (3 times), and *organizational resistance* [70] (3 times), linked to workflow changes, training requirements, and system robustness [71] (3 times). Environmental conditions pose additional challenges: low temperatures and high humidity can affect battery life and sensor accuracy on active tags, potentially causing data gaps [70].

B. BLUETOOTH ISSUES

Bluetooth and BLE devices face inherent *range limitations* (typically 10–30 meters), which require dense deployments in large storage spaces [72]. Their operation in the 2.4 GHz band also makes them susceptible to interference from Wi-Fi or other devices. Although BLE is energy efficient, frozen environments can negatively affect battery performance, forcing trade-offs between data frequency and operational life [73]. Moreover, conventional BLE deployments are typically based on central–peripheral communication and do not provide mesh operation by default. [40], limiting its suitability for large-scale distributed sensing. Bluetooth Mesh

TABLE 2. **Qualitative codebook used to classify the main *benefits* reported for each communication technology.**

Benefit category	Inclusion rule
Battery-free operation	Explicitly states that the device/tag operates without an onboard battery (e.g., passive RFID or energy-harvesting).
Low cost	Claims reduced unit or deployment cost compared to alternative technologies.
Ease of use / implementation	Reports simplified installation, configuration, or operation (e.g., minimal setup, reduced training).
Low device complexity	Describes simple hardware or firmware design, reduced component count, or minimal processing requirements.
Power efficiency	Reports low power consumption, extended battery life, or suitability for long-term operation with limited resources.
Long service life	Explicitly mentions extended operational lifetime due to passive operation, low power usage, or robust hardware design.
Scalability	Claims support for a large number of nodes/tags or easy expansion without major performance degradation.
Reliability	Reports stable operation, low packet loss, consistent read rates, or robustness of communication.
Harsh environments	Demonstrates or claims suitability for harsh conditions (e.g., low temperatures, humidity, frost, metallic environments).
Large memory capacity	Mentions increased onboard memory for data logging, history storage, or extended metadata support.
High sensitivity	Reports high receiver/tag sensitivity, improved detection capability, or enhanced read reliability at low signal levels.
Interference resistance	Explicitly addresses resistance to interference, jamming, or signal degradation due to environmental or RF conditions.
Short latency	Reports low communication delay or ability to provide near real-time data or alerts.
High data transfer speed	Claims high throughput or fast data exchange compared to other short-range technologies.
Long transmission range	Reports extended communication range relative to comparable solutions or suitability for large facilities.
Mesh networking capability	Explicitly exploits or benefits from mesh networking to extend coverage, improve redundancy, or increase reliability.
Smartphone compatibility	Reports native compatibility with smartphones or consumer devices.
Flexibility	Mentions printable, rollable, small-size, or form-factor-flexible devices suitable for diverse placements.

can address this limitation, but requires specific stack support, provisioning, and deployment planning.

Interoperability can also be an issue. Bluetooth solutions often rely on proprietary applications or middleware for data retrieval, which can hinder seamless integration into broader cold chain information systems.

C. ZigBee ISSUES

ZigBee provides scalability through mesh networking, but its performance can be affected by physical obstacles and metallic structures that attenuate signals [74]. Effective deployment may therefore require dense or carefully planned networks. Router nodes must remain powered continuously, which can be problematic in low-temperature environments where batteries perform poorly.

Large deployments may experience congestion or packet loss due to dynamic changes in network topology, especially in storage and transport scenarios where products are frequently moved. Integration with legacy systems and heterogeneous industrial platforms can further complicate widespread adoption.

D. COMMON ISSUES

Across all three technologies, interoperability with existing systems remains a persistent challenge. Cold chain networks often combine heterogeneous devices, legacy infrastructures, and fragmented data management practices [75]. Scalability is also a concern: RFID can become costly in item-level granularity, Bluetooth hubs have a limited number of concurrent connections, and ZigBee networks can experience congestion in dense deployments.

Environmental factors, including low temperatures, condensation, frost, and variable humidity, affect the propagation of wireless signals and the reliability of devices in technologies [16], [76]. Protective housings and temperature-resistant designs can mitigate these effects, but can increase costs or reduce performance.

FIGURE 11. **Word cloud of technical and operational issues associated with RFID in cold chain applications. The size of each word corresponds to the frequency with which it is cited in the relevant literature.**

IX. FUTURE TRENDS AND INNOVATIONS IN COLD CHAIN COMMUNICATION TECHNOLOGIES

The evolution of communication technologies remains a central driver of innovation in cold chain logistics. The technological challenges outlined in Section VIII constrain the practical deployment of the analyzed communication technologies, for example, which requires intermediate gateways or manual data retrieval due to their limited range. To overcome these constraints, several emerging communication trends are expected to play a pivotal role in shaping the future of cold chain monitoring. Although RFID, Bluetooth, and ZigBee represent the core solutions widely adopted today, their inherent limitations, particularly in terms of range, power consumption, and scalability, motivate the integration

TABLE 3. Qualitative codebook used to classify the main *challenges and limitations* reported for each communication technology.

Challenge category	Inclusion rule (a paper is coded if it...)
Sensor integration challenges	Reports difficulties in integrating sensing elements (e.g., chemical, temperature, humidity sensors) with communication modules, including calibration, packaging, power supply, or signal conditioning issues.
Low data security	Mentions security or privacy concerns such as weak encryption, authentication vulnerabilities, data tampering risks, or lack of secure access control.
Organizational issues	Discusses non-technical barriers such as workflow changes, staff training requirements, resistance to adoption, operational complexity, or management constraints.
High deployment cost	Reports high costs related to infrastructure, readers, gateways, network deployment, maintenance, or system integration, even when individual devices are low-cost.
Interference	Reports performance degradation due to RF interference, shared-spectrum operation, metallic or liquid environments, multipath effects, or electromagnetic noise.
Lack of global standardization	Mentions incompatibility between standards, lack of harmonized protocols, or regional differences that limit interoperability across systems or vendors.
Limited point-to-point communication	Reports the inability to support direct point-to-point links or continuous end-to-end communication without intermediate gateways or network infrastructure.
Limited data rate	Reports insufficient throughput, latency constraints, or inability to support applications requiring higher data volumes or frequent transmissions.
Low reliability / confidence	Reports unstable links, inconsistent performance, packet loss, low read rates, or limited confidence in data accuracy or system dependability.
Limited memory capacity	Mentions insufficient onboard memory for data logging, history storage, buffering, or extended metadata management.
Lack of robustness	Reports sensitivity to environmental stress (e.g., low temperatures, humidity, frost, mechanical stress) affecting device operation or communication reliability.
Short reading range	Explicitly reports limited communication or reading distance requiring dense deployments or additional infrastructure.
Unclear return on investment	States that economic benefits are uncertain, difficult to quantify, or not clearly justified compared to deployment and operational costs.
Network congestion	Reports congestion effects, packet loss, or degraded performance in dense deployments and/or under dynamic topology changes (e.g., node mobility, route reconfiguration).
Limited scalability	Reports constraints in the number of supported devices, concurrent connections (e.g., hub/central limits), or performance degradation when scaling up deployments.
Interoperability	Discusses difficulties integrating the solution with heterogeneous devices, proprietary apps/middleware, enterprise platforms, or legacy IT/logistics infrastructures.

of more advanced communication paradigms. Fig. 12 reports the yearly distribution of publications retrieved from Scopus and WoS for the three core technologies (RFID, Bluetooth and ZigBee) and for the emerging communication paradigms discussed in this section. The search was conducted using the same keyword-based procedure described in Section II. In the figure, emerging technologies are represented using lighter colors with dashed black borders, whereas the three core technologies are shown with brighter colors and no borders, in order to visually distinguish consolidated research streams from more recent trends. The results show that all emerging technologies exhibit a significantly lower number of publications compared to the three established solutions. However, 5G demonstrates a rapidly increasing trend and is progressively approaching the volume of publication of Bluetooth and ZigBee. It should also be noted that none of the emerging technologies appears in the dataset before 2019, confirming their relatively recent introduction into the cold chain. The following subsections expand the discussion by explicitly comparing these emerging technologies with the existing core solutions.

A. INTEROPERABILITY OF COMMUNICATION PROTOCOLS

Next-generation cold chain systems are increasingly hybrid, integrating multiple wireless standards into cohesive networks. Rather than relying on a single protocol, modern IoT architectures combine short-range sensors with long-range backhaul (such as LPWAN or cellular) through multi-protocol gateways. This convergence ensures continuous coverage across diverse environments: for example, an RFID or Bluetooth sensor inside a container can transmit its data via a Long Range Wide Area Network (LoRaWAN), Narrowband-IoT NB-IoT, or Long Term Evolution/5G link when out of range of local readers. In this context, the emerging technologies complement the core ones by overcoming their range limitations: whereas RFID, Bluetooth, and ZigBee are restricted to short-range communication, LPWAN and cellular links extend connectivity across entire logistics chains. By dynamically selecting the best available channel based on range, power, and bandwidth needs, such interoperable frameworks overcome the fragmentation and interoperability issues that traditionally hinder IoT deployments. The result is a more resilient cold chain communication infrastructure in which heterogeneous devices seamlessly share data.

B. LOW-POWER WIDE AREA NETWORKS (LPWAN)

Ultra-low-power, long-range networks have become pivotal for connecting distant or mobile cold chain assets. Protocols like LoRaWAN, Sigfox, Long Term Evolution for Machines, and NB-IoT enable near-real-time telemetry over kilometers while consuming minimal energy. [77] Compared with Bluetooth and ZigBee, which operate at short range and require

TABLE 4. Comparison of core and emerging communication technologies for cold chain monitoring.

Technology	Typical Range	Power Consumption	Data Rate	Localization Accuracy	Scalability	Suitable Use Cases
RFID (UHF)	Short (meters)	Very low / passive	Low	Low–medium	Medium	Item-level tagging, package-level temperature tracking, inventory checkpoints
Bluetooth / BLE	Short (5–30 m)	Low	Medium	Medium	Medium	Pallet monitoring, warehouse sensing, proximity-based alerts
ZigBee	Short/medium (10–100 m)	Low	Medium	Medium	High (mesh)	Warehouse sensor networks, container-level monitoring, mesh deployments
LoRaWAN	Long (km)	Very low	Very low	Low	Very high	Long-haul logistics, refrigerated trucks, remote storage sites
NB-IoT	Long (km)	Low–medium	Low–medium	Low	Very high	Cross-border shipments, real-time visibility over cellular networks
5G (mMTC/URLLC)	Short/medium (cells)	Medium	High–very high	High	Very high	High-bandwidth monitoring, real-time alarms, autonomous refrigeration control
UWB	Short (10–50 m)	Medium	High	Very high (cm-level)	Low–medium	High-precision indoor localization in warehouses and pharma facilities

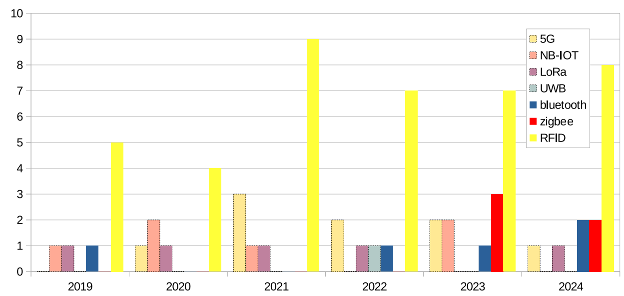

FIGURE 12. Number of articles indexed by Scopus and WoS per year mentioning one between “cold chain” or “cool chain” and one of the considered technologies.

denser reader infrastructures, LPWAN technologies support kilometer-scale communication with far lower maintenance demands. These LPWAN technologies help mitigate range and infrastructure-density limitations of high power draw and coverage, making them ideal for battery-powered refrigerated trucks, remote storage sites, or trans-border shipments. For example, NB-IoT and LoRa devices can transmit temperature data from insulated containers over wide areas without frequent battery changes.

C. ULTRA-WIDEBAND (UWB) AND 5G

For certain cold chain use-cases, communication demands are shifting toward higher accuracy and bandwidth. UWB technology, known for its precise range capability, is being tested in cold chain asset tracking where pinpoint indoor location is crucial. UWB-based real-time locating systems have been reported to achieve sub-meter accuracy in indoor cold-chain or pharmaceutical-like storage scenarios, depending on deployment geometry and environmental conditions. This positional accuracy far surpasses that of Bluetooth or ZigBee beacons, enabling more efficient retrieval and management of goods in large storage sites.

Meanwhile, 5G wireless is expected to provide the high-throughput, low-latency backbone required for data-intensive cold chain applications. [78] Unlike the core technologies, whose bandwidth and latency constraints limit certain real-time applications, 5G supports massive device connectivity and ultra-reliable low-latency links, opening the door to advanced services such as autonomous refrigeration control and predictive analytics. For example, recent prototypes for shipborne cold chain monitoring integrate 5G modules into multi-sensor acquisition systems, combining temperature and humidity sensors with IoT cloud platforms to ensure fast data transmission even under harsh maritime conditions [79]. Testing shows that such 5G-enabled systems achieve high transmission rates and low packet loss, meeting the real-time information transmission requirements of the shipborne cold chain industry.

D. ENERGY HARVESTING AND BATTERY-FREE SENSORS

A push toward battery-free sensor tags is underway to reduce maintenance and enable deployments in tighter spaces (e.g., inside packages or vaccine vials). Passive UHF RFID tags are a prime example: they harvest energy from a reader’s radio waves, and thus operate battery-free, making them inexpensive and compact. This concept has been applied to create flexible wireless temperature sensors that can be inserted directly into products. Recent work demonstrates a fully battery-free temperature tag, printed on a thin, flexible substrate capable of continuous cold storage monitoring, powered purely by the interrogating RFID reader's signal. These advances extend the legacy of RFID-based sensing while complementing Bluetooth- and ZigBee-based solutions, which typically require on-board power and thus more frequent maintenance. Such tags leverage ambient energy (RF backscatter or even light/vibration) to communicate without onboard power, allowing ''place-and-forget'' sensor deployments.

E. SECURITY AND AUTHENTICATION PROTOCOLS

A comprehensive and technology-specific analysis of security threats and countermeasures for RFID, Bluetooth, and ZigBee can be found in dedicated survey studies available in the literature. Although these works are not explicitly focused on cold chain applications, they provide a detailed and structured examination of attack models, vulnerabilities, and mitigation strategies that are directly applicable to cold chain communication systems. In particular, high quality surveys for RFID [80], Bluetooth [81], and ZigBee [82] offer an in-depth treatment of protocol-layer threats, cryptographic mechanisms, authentication schemes, and system-level countermeasures relevant to resource-constrained IoT environments.

At the physical layer, RFID systems are vulnerable to tag removal or destruction, relay attacks, and intentional jamming, all of which are particularly critical in cold chain logistics, where tag availability directly affects traceability and compliance. At the network transport layer, cloning, spoofing, and eavesdropping attacks exploit weak or absent authentication mechanisms, potentially allowing unauthorized replication of tag identities or interception of temperature and logistics data. Application-layer threats include unauthorized tag reading, tag memory modification, and middleware vulnerabilities such as buffer overflow attacks, which may compromise backend logistics platforms and the integrity of monitoring records.

Countermeasures proposed in the literature include challenge–response authentication protocols to mitigate cloning and replay attacks, encrypted communication channels to prevent passive eavesdropping, secure key management practices, and the use of strong cryptographic primitives compliant with open standards. Lightweight cryptographic mechanisms are particularly relevant in RFID environments due to the severe resource constraints of passive tags. Additional protections such as intrusion detection systems, anti-brute-force mechanisms, nonces and sequence numbers for replay resistance, and electromagnetic shielding against side-channel exploitation further enhance robustness. In regulated cold chain scenarios, where traceability and data integrity have legal implications, these security measures are not optional enhancements, but fundamental architectural requirements.

As IoT-based cold chain systems scale in size and complexity, data security, authenticity, and integrity become critical design requirements. Temperature and environmental measurements are not just operational data; in regulated sectors such as food and pharmaceuticals, they directly support compliance, traceability, and liability assessment. Consequently, communication technologies must ensure data confidentiality, integrity, and authenticated access.

At the protocol level, the three core technologies present different security characteristics and constraints. RFID systems, particularly passive tags, often operate under strict energy and hardware limitations, which can restrict the adoption of advanced cryptographic primitives and expose them to risks such as cloning or unauthorized reading. Bluetooth Low Energy incorporates pairing, authentication, and encryption mechanisms, yet its security level is strongly dependent on configuration choices and key management practices. ZigBee integrates AES-128 encryption and network key distribution mechanisms; however, mesh architectures introduce additional considerations regarding key propagation and node trust models.

Bluetooth-based systems are exposed to a heterogeneous threat landscape spanning physical, protocol, and application layers. Common risks include passive eavesdropping, address spoofing (BD_ADDR manipulation), relay and reflection attacks, and man-in-the-middle (MITM) exploits during the pairing procedure. In particular, association models that do not enforce authenticated key exchange (e.g., ''Just Works'') provide limited protection against active interception. Additional vulnerabilities may arise from weak PIN selection, insufficient entropy in negotiated encryption keys, insecure storage of long-term keys, or fallback to lower security modes for legacy compatibility. Denial-of-service vectors, including battery-draining attacks and channel jamming, are also relevant in resource-constrained devices. Beyond protocol-level issues, implementation flaws in profile authorization, operating system integration, and user interface design can further enlarge the attack surface, enabling unauthorized data access or device control even when cryptographic primitives are formally enabled.

Addressing these risks requires a layered security approach combining protocol hardening, secure implementation practices, and operational governance. From a technical standpoint, authenticated pairing mechanisms (e.g., passkey-based or ECDH-based key exchange) should be enforced, minimum encryption key lengths must be guaranteed, and secure storage mechanisms should protect long-term credentials. Devices should avoid insecure fallback modes and restrict discoverability when not required. Firmware updates and vulnerability management are essential to mitigate newly disclosed protocol weaknesses. At the system level, monitoring mechanisms capable of detecting anomalous BLE traffic patterns can reduce exposure to active attacks. Where regulatory compliance or data integrity requirements are stringent, application-layer end-to-end encryption should complement link-layer security to prevent intermediate exposure. Finally, structured key lifecycle management (provisioning, rotation, revocation) and operator awareness programs are necessary to ensure that security controls remain effective throughout deployment.

ZigBee inherits a layered security architecture based on IEEE 802.15.4 link-layer protection and ZigBee network and application-layer mechanisms, but practical deployments remain exposed to a broad spectrum of vulnerabilities. The predominant issues concern key management and trust assumptions: a single network key often protects all devices in a PAN, commissioning procedures may still rely on default or globally known trust-center link keys, and key-transport messages can be exposed to passive eavesdropping or active manipulation. Once a network key is recovered, an adversary can decrypt traffic, inject forged commands, or silently join the network. In addition, the use of shared cryptographic material and limited replay protection makes ZigBee networks susceptible to replay and ‘‘ghost’’ attacks, in which bogus frames trigger expensive security processing and accelerate battery depletion. At the network layer, routing and topology-control mechanisms enable more structural attacks such as wormhole, sinkhole, and Sybil attacks, which can reroute traffic through malicious relays, disrupt connectivity, or create the illusion of many fictitious nodes. PAN ID conflicts, association flooding, and crafted management frames further enable denial-of-service conditions, especially in dense or resource-constrained deployments. These protocol-level weaknesses are compounded by implementation choices: legacy devices that predate stronger security options and low-cost products that ship with minimal security configuration significantly enlarge the attack surface.

Mitigation strategies and design implications. Improving the security posture of ZigBee-based systems requires hardening both the protocol configuration and the deployment practices. At the cryptographic level, use of pre-shared global keys and default trust-center link keys should be avoided; instead, devices should employ unique installation codes or per-device link keys, authenticated key establishment, and systematic key rotation. Network security modes should be configured to enforce encryption and integrity protection for both network and application traffic, with replay protection correctly implemented and monitored. From an architectural perspective, trust-center policies should restrict which devices may join, validate address and identity claims to counter Sybil-style attacks, and limit the impact of a compromised node through fine-grained authorization. To address DoS and energy-depletion attacks, rate limiting, anomaly detection (e.g., for repeated association attempts or abnormal management traffic), and robust buffer management strategies are needed, particularly on coordinators and routers. Finally, given the long lifetime of many ZigBee devices, secure firmware-update mechanisms and deprecation strategies for legacy, weakly protected nodes are essential to prevent old vulnerabilities from undermining otherwise robust cold-chain deployments.

In regulated cold chain environments, data integrity and auditability are not only technical concerns but regulatory obligations. Electronic records must remain tamper-resistant, traceable, and attributable to authenticated devices or operators. For this reason, research efforts increasingly focus on lightweight cryptographic algorithms tailored to low-power IoT nodes, secure key exchange protocols, and end-to-end encrypted data pipelines.

In parallel, distributed ledger technologies are being explored to reinforce integrity and non-repudiation properties in cold chain monitoring systems. Blockchain-based architectures can provide tamper-evident storage of environmental logs and improve trust among multiple stakeholders operating on heterogeneous infrastructures [83].

These security frameworks become even more relevant as systems evolve from localized deployments based on RFID, Bluetooth, or ZigBee to large-scale heterogeneous networks integrating LPWAN and 5G backhaul. The expansion of connectivity increases the attack surface and highlights the importance of scalable identity management, secure interoperability, and robust authentication mechanisms across multi-protocol ecosystems.

X. IMPLICATIONS FOR TECHNOLOGY SELECTION IN COLD CHAIN SYSTEMS

The bibliometric and qualitative characterization of RFID, Bluetooth, and ZigBee research presented in the previous sections does not account for economic aspects, such as Total Cost of Ownership (TCO), and Return on Investment (ROI), nor for performance metrics, such as data rate and localization accuracy. Indeed, the existing literature reports these parameters in a highly heterogeneous manner. The available data are typically context-specific (pilot deployment, laboratory prototype, or industrial implementation), often incomplete with respect to infrastructure, maintenance, and integration components, and rarely standardized or supported by comparable evaluation methodologies. Despite these limitations, this section aims to provide practitioners with actionable criteria for aligning technology choices with operational requirements. To this end, it derives decision-oriented guidance from the benefits and challenges synthesized in Sections VII and VIII, as well as from the cold chain stage analysis in Section IV. Given the heterogeneity of the surveyed literature and the prevalence of qualitative claims rather than harmonized metrics, the following guidelines should be interpreted as a practical synthesis of recurrent patterns, rather than as a quantitative benchmarking.

A. KEY DECISION DRIVERS

Across cold chain applications, technology selection is primarily driven by a combination of (i) identification granularity, (ii) required communication range and infrastructure density, (iii) power and maintenance constraints, (iv) environmental harshness and interference conditions, and (v) interoperability and security requirements.

Granularity and traceability. When item-level identification or checkpoint-based traceability is the main objective (e.g., pallet/carton identification at warehouse gates or distribution hubs), RFID is the most natural solution due to its low-cost tags and battery-free operation. Conversely, when continuous sensing and near-real-time telemetry is required (e.g., continuous temperature logging inside cold rooms or transport units), Bluetooth and ZigBee-based architectures are more frequently adopted because they support sensor nodes with periodic transmissions and integration with gateways or mobile devices.

Coverage and infrastructure constraints. Bluetooth typically supports short-range communication and, therefore, benefits from dense deployments in large facilities, with a frequent reliance on smartphones or local gateways for data retrieval. ZigBee extends coverage through mesh networking, which is advantageous for warehouses or storage environments where multi-hop topologies can reduce the need for direct long-range links. RFID read ranges depend on tag type, frequency, and environment, and are often adequate for portals, checkpoints, and inventory tasks but less suited to continuous multi-hop coverage.

Power, maintenance, and temperature effects. Passive RFID tags provide a strong advantage in scenarios where battery replacement is impractical, but this comes at the cost of infrastructure dependence on readers and sensitivity to materials (e.g., liquids, metals, ice). Bluetooth and ZigBee nodes often require batteries or continuous power; low temperatures and frost can reduce battery performance and, therefore, impose design trade-offs between transmission rate and operational lifetime.

Interference and robustness. All three technologies may suffer from degraded performance in cold chain environments due to condensation, metallic structures, dense packaging, or RF coexistence. RFID is frequently reported to be sensitive to interference in the presence of liquids/metal and to installation constraints, while Bluetooth may be affected by congestion of the 2.4 GHz band (e.g., Wi-Fi coexistence). ZigBee performance can degrade in the presence of obstacles and may require careful network planning to prevent congestion in dense deployments.

Integration, security, and organizational adoption. Interoperability with enterprise systems and across supply-chain actors remains a recurring barrier, along with security concerns and organizational issues such as training and process changes. In practice, solutions that rely on proprietary middleware or closed ecosystems may hinder data continuity across cold chain stages, even if the underlying communication link is reliable.

B. REPRESENTATIVE DEPLOYMENT SCENARIOS

To illustrate how these decision drivers map to practical deployments, three representative scenarios are summarized below. These examples are derived from recurring application patterns observed in the surveyed literature and aligned with stage taxonomy.

1) ITEM-LEVEL TRACEABILITY AND CHECKPOINT MONITORING (RFID)

A common deployment pattern in distribution centers and retail backrooms relies on RFID tags attached to pallets, cartons, or individual items. Fixed or handheld readers at checkpoints (e.g., warehouse gates, loading/unloading points) automate identification and can support temperature sensing when sensor-equipped tags are used. This approach is attractive when low-cost, battery-free tagging and rapid identification are required. However, the literature repeatedly highlights the sensitivity to interference and material effects (e.g., metal, moisture, ice), and infrastructure costs associated with readers, antenna placement, and integration into logistics IT systems. In such settings, antenna design, placement optimization, and standard compliance are often decisive for robustness.

2) LOCAL MONITORING WITH HUMAN-IN-THE-LOOP ACCESS (BLUETOOTH)

Bluetooth solutions are frequently adopted for short-range monitoring, where operators can retrieve data using smartphones or where a local gateway periodically collects logs. Typical examples include pallet monitoring during handling operations, cold room inspections, and last-mile segments where rapid access to temperature history is needed without dedicated RFID readers. The smartphone compatibility and low energy operation of BLE simplify deployment and maintenance. The main limitations are short range, coexistence/interference in the 2.4 GHz band, and the need to balance sampling/transmission frequency against battery lifetime in low-temperature environments. This scenario fits well when operational processes already include personnel interaction (loading/unloading, inspection routines), but becomes less effective for fully autonomous end-to-end monitoring.

3) DISTRIBUTED SENSING INFRASTRUCTURE IN WAREHOUSES (ZIGBEE)

ZigBee is typically used for distributed monitoring in cold warehouses and storage facilities, where multiple sensor nodes measure temperature/humidity and transmit data through a mesh network to a coordinator or gateway. The mesh capability supports scalability and coverage extension without requiring each node to directly reach the gateway. This approach is effective for facilities with stable layouts and continuous monitoring needs, but requires careful planning of router placement and power availability, and may experience congestion or reduced reliability in dense deployments or highly dynamic environments. Integration with existing platforms is also a recurring issue, especially when heterogeneous devices and legacy infrastructures coexist.

C. PRACTICAL SELECTION GUIDANCE

Based on the above patterns, the following guidance summarizes the typical fit of each technology:

- **Prefer RFID** when the primary goal is *identification and traceability at checkpoints* (item/pallet level), when *battery-free tags* are desirable, and when infrastructure-based reading is acceptable. Pay particular attention to interference/material effects and to reader/antenna configuration.
- **Prefer Bluetooth/BLE** when *short-range sensing with easy access* is required (e.g., via smartphones), when deployments benefit from human interaction or local gateways, and when energy efficiency is critical. Range and 2.4 GHz coexistence should be explicitly managed, especially in large facilities.
- **Prefer ZigBee** for *warehouse-scale distributed monitoring* requiring mesh scalability and continuous sensing, particularly in stable infrastructures where router placement and power can be engineered. Network planning and congestion management are important for reliability.

Finally, the bibliometric evidence suggests that emerging paradigms (e.g., LPWAN and 5G backhaul) are increasingly investigated to complement short-range solutions. In practice, hybrid architectures that combine local sensing (RFID/Bluetooth/ZigBee) with long-range backhaul via gateways can mitigate range limitations and improve end-to-end visibility across cold chain stages, while preserving the cost and energy advantages of short-range technologies.

XI. CONCLUSION

RFID, Bluetooth, and ZigBee have become key enablers of digital cold chain monitoring, each providing specific strengths in terms of identification, sensing, communication range, and deployment flexibility. The bibliometric analysis highlights the distinct disciplinary emphases and research trends associated with each technology, reflecting differences in maturity, application scope, and integration requirements.

Despite their benefits, all three technologies face operational challenges, including signal interference, environmental harshness, range limitations, power constraints, and interoperability issues. Addressing these limitations requires careful system design and the adoption of emerging communication paradigms.

Recent developments suggest a shift toward integrated IoT architectures that combine short-range communication technologies with long-range LPWAN or cellular links, supported by cloud platforms and multi-protocol gateways. Emerging solutions such as 5G, UWB, battery-free sensors, and blockchain have the potential to expand coverage, improve reliability, and strengthen data integrity throughout the supply chain.

Future research should continue to explore scalable, secure and energy-efficient communication frameworks capable of supporting the increasing complexity and global reach of cold chain logistics. Such advances will contribute to improving the integrity of the product, reducing waste, and improving operational transparency.

REFERENCES

[1] M. M. Aung and Y. S. Chang, *Cold Chain Management*. Cham, Switzerland: Springer, 2023.

[2] L. Bai, M. Liu, and Y. Sun, "Overview of food preservation and traceability technology in the smart cold chain system," *Foods*, vol. 12, no. 15, p. 2881, Jul. 2023.

[3] Y. B. Yu, K. T. Briggs, M. B. Taraban, R. G. Brinson, and J. P. Marino, "Grand challenges in pharmaceutical research series: Ridding the cold chain for biologics," *Pharmaceutical Res.*, vol. 38, no. 1, pp. 3–7, Jan. 2021.

[4] Y. Wang, Y. Li, Q. Lu, J. Zhang, X. Zhang, Z. Ding, and H. Xu, "Research on evolutionary game of pharmaceutical supply chain platform considering government supervision behavior," *IEEE Access*, vol. 12, pp. 143930–143944, 2024.

[5] *WHO Technical Report Series, no. 961: Annex 9: Model Guidance for the Storage and Transport of Time- and Temperature-Sensitive Pharmaceutical Products*, World Health Organization, Geneva, Switzerland, 2011.

[6] J.-W. Han, L. Ruiz-Garcia, J.-P. Qian, and X.-T. Yang, "Food packaging: A comprehensive review and future trends," *Comprehensive Rev. Food Sci. Food Saf.*, vol. 17, no. 4, pp. 860–877, Jul. 2018.

[7] J.-W. Han, M. Zuo, W.-Y. Zhu, J.-H. Zuo, E.-L. Lü, and X.-T. Yang, "A comprehensive review of cold chain logistics for fresh agricultural products: Current status, challenges, and future trends," *Trends Food Sci. Technol.*, vol. 109, pp. 536–551, Mar. 2021.

[8] N. Dilillo, R. Ferrero, F. Gandino, and M. Rebaudengo, "Investigation on wireless communication for sensors in IoT cold chain," in *Proc. IEEE Conf. AgriFood Electron. (CAFE)*, Sep. 2023, pp. 89–93.

[9] A. D. Sánchez, M. de la Cruz Del Río Rama, and J. Á. García, "Bibliometric analysis of publications on wine tourism in the databases scopus and WoS," *Eur. Res. Manage. Bus. Econ.*, vol. 23, no. 1, pp. 8–15, Jan. 2017.

[10] S. Echchakoui, "Why and how to merge scopus and web of science during bibliometric analysis: The case of sales force literature from 1912 to 2019," *J. Marketing Anal.*, vol. 8, no. 3, pp. 165–184, Sep. 2020.

[11] S. Mercier, S. Villeneuve, M. Mondor, and I. Uysal, "Time–temperature management along the food cold chain: A review of recent developments," *Comprehensive Rev. Food Sci. Food Saf.*, vol. 16, no. 4, pp. 647–667, Jul. 2017.

[12] E. Abad, F. Palacio, M. Nuin, A. G. D. Zárate, A. Juarros, J. M. Gómez, and S. Marco, "RFID smart tag for traceability and cold chain monitoring of foods: Demonstration in an intercontinental fresh fish logistic chain," *J. Food Eng.*, vol. 93, no. 4, pp. 394–399, Aug. 2009.

[13] M. Grunow and S. Piramuthu, "RFID in highly perishable food supply chains—Remaining shelf life to supplant expiry date?" *Int. J. Prod. Econ.*, vol. 146, no. 2, pp. 717–727, Dec. 2013.

[14] A. Carullo, S. Corbellini, M. Parvis, and A. Vallan, "A wireless sensor network for cold-chain monitoring," *IEEE Trans. Instrum. Meas.*, vol. 58, no. 5, pp. 1405–1411, May 2009.

[15] L. Ruiz-Garcia, L. Lunadei, P. Barreiro, and I. Robla, "A review of wireless sensor technologies and applications in agriculture and food Industry: State of the art and current trends," *Sensors*, vol. 9, no. 6, pp. 4728–4750, Jun. 2009.

[16] R. Badia-Melis, U. Mc Carthy, L. Ruiz-Garcia, J. Garcia-Hierro, and J. I. R. Villalba, "New trends in cold chain monitoring applications—A review," *Food Control*, vol. 86, pp. 170–182, Apr. 2018.

[17] P. H. Chou, C.-T. Lee, Z.-Y. Peng, J.-P. Li, T. K. Lai, C.-M. Chang, C.-H. Yang, Y.-L. Chen, C.-C. Nien, L.-H. Chen, L.-Y. Lai, J.-C. Lu, and S.-C. Hung, "A Bluetooth-smart insulating container for cold-chain logistics," in *Proc. IEEE 6th Int. Conf. Service-Oriented Comput. Appl. (SOCA)*, Mar. 2013, pp. 298–303.

[18] S. Jiang, S. Jia, and H. Guo, "Internet of Things (IoT)-enabled framework for a sustainable vaccine cold chain management system," *Heliyon*, vol. 10, no. 7, Apr. 2024, Art. no. e28910.

[19] J. Gillespie, T. P. da Costa, X. Cama-Moncunill, T. Cadden, J. Condell, T. Cowderoy, E. Ramsey, F. Murphy, M. Kull, R. Gallagher, and R. Ramanathan, "Real-time anomaly detection in cold chain transportation using IoT technology," *Sustainability*, vol. 15, no. 3, p. 2255, Jan. 2023.

[20] V. Raab, B. Petersen, and J. Kreyenschmidt, "Temperature monitoring in meat supply chains," *Brit. Food J.*, vol. 113, no. 10, pp. 1267–1289, Sep. 2011.

[21] Y.-Y. Chen, Y.-J. Wang, and J.-K. Jan, "A novel deployment of smart cold chain system using 2G-RFID-sys," *J. Food Eng.*, vol. 141, pp. 113–121, Nov. 2014.

[22] H. Kim, H. Jeong, and H. Park, "A study on RFID/USN based e-pedigree system for cold chain management," in *Proc. Int. Technol. Manage. Conf.*, Jun. 2012, pp. 137–143.

[23] M. Trebar, M. Lotrič, and I. Fonda, "Use of RFID temperature monitoring to test and improve fish packing methods in styrofoam boxes," *J. Food Eng.*, vol. 159, pp. 66–75, Aug. 2015.

[24] X. Li and L. Huo, "Study on logistics information packaging technology of fresh food in cold chain," in *Advanced Graphic Communications, Packaging Technology and Materials*. Cham, Switzerland: Springer, 2016, pp. 579–584.

[25] M. Xue, "Research on cold storage environment monitoring system based on ZigBee," in *Proc. Int. Conf. Signal Process. Commun. Secur. (ICSPCS)*, Jul. 2024, p. 17.

[26] L. Kai, W. Gao, and C. Cong, "Oyster cold chain logistics monitoring system based on RFID and cloud platforms," in *Proc. 4th Int. Conf. Signal Process. Comput. Sci. (SPCS)*, Dec. 2023, p. 36.

[27] L. Huihui, L. Na, and K. Qingqing, "Research on green cold chain logistics information system under computer big data," in *Proc. Int. Conf. Comput., Inf. Process. Adv. Educ. (CIPAE)*, Aug. 2023, pp. 83–87.

[28] X. Zong and H. Shao, "Design of cold chain logistics remote monitoring system based on ZigBee and GPS location," *AIP Conf. Proc.*, vol. 1820, Mar. 2017, Art. no. 090013.

[29] H. Jiang, F. Jiang, and Z. Chen, "Green cold chain logistics routing optimization based on chaotic mechanism hybrid SSA algorithm with fuzzy time window multi- objective multi-distribution center," *IEEE Access*, vol. 12, pp. 141540–141558, 2024.

[30] X. Yang and H. Jiang, "Research on urban cold chain logistics path optimization considering multi-center and time-varying road networks," *IEEE Access*, vol. 12, pp. 71331–71348, 2024.

[31] M. Ghazal, H. Anan, and S. Mejjaouli, "Transportation of perishable goods & rerouting solutions," in *Proc. 3rd Int. Conf. Ind. Eng. Ind. Manage.*, Jan. 2022, pp. 207–213.

[32] C. Du, J. Sun, and Y. Fan, "Research on the whole process information system of cold chain supply in artificial intelligence logistics enterprises," in *Proc. IEEE 3rd Int. Conf. Data Sci. Comput. Appl. (ICDSCA)*, Oct. 2023, pp. 1092–1096.

[33] B. S. Kim, J. Y. Kim, J. H. Kim, H. O. Lee, Y. J. Lee, S. Mezemir, J. Koo, J. Y. Jung, and H. J. Kim, "Quality monitoring in cold-chain of leafy vegetables converging ICT," in *Proc. 4th IIR Int. Conf. Sustainability Cold Chain*, 2016, pp. 421–428.

[34] H. Zhou, "Application of RFID information technology in fresh food cold chain logistics management," *J. Phys., Conf. Ser.*, vol. 1881, no. 3, Apr. 2021, Art. no. 032002.

[35] A. S. Martínez-Sala, E. Egea-López, F. García-Sánchez, and J. García-Haro, "Tracking of returnable packaging and transport units with active RFID in the grocery supply chain," *Comput. Ind.*, vol. 60, no. 3, pp. 161–171, Apr. 2009.

[36] C. D. Bui, A. Quinn, D. Iacopino, and A. Narbudowicz, "Compact chipless RFID sensor for frozen food monitoring," *IEEE Sensors J.*, vol. 24, no. 9, pp. 14205–14212, May 2024.

[37] W. Li-Feng, H. Fei, and G.-H. Zhu, "Design of cold chain logistics information real time tracking system based on wireless RFID technology," in *Proc. Int. Conf. Adv. Hybrid Inf. Process.*, in Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 416, 2022, pp. 440–453.

[38] Y. Shafiq, J. Henricks, C. P. Ambulo, T. H. Ware, and S. V. Georgakopoulos, "A battery-free temperature sensor with liquid crystal elastomer switching between RFID chips," *IEEE Access*, vol. 8, pp. 87870–87883, 2020.

[39] W. Qiu, "Design of cold chain storage and transportation monitoring system for fresh agricultural products based on artificial intelligence," in *Proc. IEEE 3rd Int. Conf. Electr. Eng., Big Data Algorithms (EEBDA)*, Feb. 2024, pp. 1402–1406.

[40] L. Chen, J. Zhang, X. Tang, and Q. Gao, "A remote monitoring system for cold chain logistics by means of social networks," *Open Cybern. Systemics J.*, vol. 9, no. 1, pp. 888–893, Aug. 2015.

[41] J. Tian, "Research on logistics cold chain system based on computer 3D intelligent electrical remote control," in *Proc. 5th Int. Conf. Artif. Intell. Comput. Appl. (ICAICA)*, Nov. 2023, pp. 686–690.

[42] W.-J. Liao, T.-W. Lien, B.-R. Hsiao, H.-S. Wang, C.-F. Yang, J.-H. Tarng, C.-C. Nien, and T.-C. Chiu, "Sensor integrated antenna design for applications in cold chain logistic services," *IEEE Trans. Antennas Propag.*, vol. 63, no. 2, pp. 727–735, Feb. 2015.

[43] Z. Huang and C. Liu, "Improvement of UHF RFID detection rate in multipath environment using beam-switching antenna array," in *IEEE MTT-S Int. Microw. Symp. Dig.*, May 2022, pp. 156–158.

[44] A. M. J. Marindra, B. M. Pratama, and D. J. Suroso, "Non-invasive frozen meat monitoring system using UHF RFID tag antenna-based sensing and RSSI," *Int. J. Adv. Sci., Eng. Inf. Technol.*, vol. 13, no. 1, pp. 1–7, Jan. 2023.

[45] L. Xinyu, C. Fuyin, L. Mai, and S. Ying, "Tuna cryogenic cold chain transport solution based on quorum sensing intelligence," in *Proc. 4th Int. Conf. Control Robot. (ICCR)*, Dec. 2022, pp. 174–178.

[46] L. Qi, Y. Han, X. Zhang, S. Xing, and Z. Fu, "Real time monitoring system for aquatic cold-chain logistics based on WSN," *Trans. Chin. Soc. Agricult. Machinery*, vol. 43, no. 8, pp. 134–140, 2012.

[47] L. K. Baghel, R. Raina, S. Kumar, and L. Catarinucci, "IoT-based integrated sensing and logging solution for cold chain monitoring applications," *IEEE J. Radio Freq. Identificat.*, vol. 8, pp. 837–846, 2024.

[48] D. Valderas, F. Villa-González, R. Bhattacharyya, and S. Sarma, "Time–temperature excursion monitoring using chipless RFID tags and organic oils," *IEEE Sensors J.*, vol. 23, no. 17, pp. 19028–19036, Sep. 2023.

[49] A. Soylemezoglu, M. J. Zawodniok, and S. Jagannathan, "RFID-based smart freezer," *IEEE Trans. Ind. Electron.*, vol. 56, no. 7, pp. 2347–2356, Jul. 2009.

[50] A. U. Khan, Y. Ali, D. Pamucar, and L. Vasa, "Risk management for cold supply chain: Case of a developing country," *Acta Polytechnica Hungarica*, vol. 19, no. 8, pp. 161–185, 2022.

[51] S. Guo, "Exploring the application of multi-objective optimization algorithms in logistics sensor networks," in *Proc. 2nd Int. Conf. Inventive Comput. Informat. (ICICI)*, Jun. 2024, pp. 644–650.

[52] I. Masudin, A. Ramadhani, D. P. Restuputri, and I. Amallynda, "The effect of traceability system and managerial initiative on Indonesian food cold chain performance: A COVID-19 pandemic perspective," *Global J. Flexible Syst. Manage.*, vol. 22, no. 4, pp. 331–356, Dec. 2021.

[53] F. Villa-Gonzalez, R. Bhattacharyya, T. Athauda, S. E. Sarma, and N. C. Karmakar, "Detecting breaks in cold chain integrity using chipless RFID time–temperature sensors," *IEEE Sensors J.*, vol. 22, no. 18, pp. 17808–17818, Sep. 2022.

[54] X. Zhang, Z. Lin, J. Guo, and Y. Zhang, "Information fusion-based temperature sensing with passive UHF RFID tags," *IEEE Sensors Lett.*, vol. 8, no. 10, pp. 1–4, Oct. 2024.

[55] I. Masudin, A. Ramadhani, and D. P. Restuputri, "Traceability system model of Indonesian food cold-chain Industry: A COVID-19 pandemic perspective," *Cleaner Eng. Technol.*, vol. 4, Oct. 2021, Art. no. 100238.

[56] O. Urbano, A. Perles, C. Pedraza, S. Rubio-Arraez, M. L. Castelló, M. D. Ortola, and R. Mercado, "Cost-effective implementation of a temperature traceability system based on smart RFID tags and IoT services," *Sensors*, vol. 20, no. 4, p. 1163, Feb. 2020.

[57] Y. Li, Y. Peng, L. Zhang, J. Wei, and D. Li, "Quality monitoring traceability platform of agriculture products cold chain logistics based on the Internet of Things," *Chem. Eng. Trans.*, vol. 46, pp. 517–522, Jan. 2015.

[58] K. Yang, U. Botero, H. Shen, D. L. Woodard, D. Forte, and M. M. Tehranipoor, "UCR: An unclonable environmentally sensitive chipless RFID tag for protecting supply chain," *ACM Trans. Design Autom. Electron. Syst.*, vol. 23, no. 6, pp. 1–24, Nov. 2018.

[59] F. Li and Z. Chen, "Brief analysis of application of RFID in pharmaceutical cold-chain temperature monitoring system," in *Proc. Int. Conf. Transp., Mech., Electr. Eng. (TMEE)*, Dec. 2011, pp. 2418–2420.

[60] N. D'Uva, F. Camera, S. Amendola, S. Nappi, C. Miozzi, C. Occhiuzzi, and G. Marrocco, "Batteryless wireless temperature/humidity sensor for item-level smart pharma packaging," in *Proc. IEEE Int. Workshop Metrology Ind. 4.0 IoT*, Jun. 2021, pp. 145–149.

[61] S. Gautam and S. Kumar, "RTOS based data logger using BLE periodic advertising for cold chain temperature monitoring," in *Proc. IEEE 99th Veh. Technol. Conf. (VTC-Spring)*, Jun. 2024, pp. 01–07.

[62] H. Luo, M. Zhu, S. Ye, H. Hou, Y. Chen, and L. Bulysheva, "An intelligent tracking system based on Internet of Things for the cold chain," *Internet Res.*, vol. 26, no. 2, pp. 435–445, Apr. 2016.

[63] C. Liu, R. Zhang, I. Chen, and T. Yi, "The WSN real-time monitoring system for agricultural products cold-chain logistics," in *Proc. Int. Conf. Comput. Comput. Technol. Agricult.*, in IFIP Advances in Information and Communication Technology, vol. 420, 2014, pp. 225–261.

[64] J. Diao, P. Sun, J. Chen, Z. Zhang, and Z. Chen, "Intelligent medicine box monitoring system based on ZigBee technology," in *Proc. Int. Conf. Power Electron. Artif. Intell.*, Jan. 2024, pp. 924–928.

[65] L. Ruiz-Garcia, P. Barreiro, J. I. Robla, and L. Lunadei, "Testing ZigBee motes for monitoring refrigerated vegetable transportation under real conditions," *Sensors*, vol. 10, no. 5, pp. 4968–4982, May 2010.
[66] P. Hongmin, "Design of cold chain logistics monitoring system based on ZigBee and GPS positioning technology," in *Proc. 3rd Int. Conf. Smart Gener. Comput., Commun. Netw. (SMART GENCON)*, Dec. 2023, pp. 1–5.
[67] M. Laniel and J.-P. Émond, "Mapping of RFID tag readability in relation to the food content in a refrigerated sea container at 915 MHz," *Innov. Food Sci. Emerg. Technol.*, vol. 11, no. 4, pp. 703–706, Oct. 2010.
[68] A. Singh, A. Gutub, A. Nayyar, and M. K. Khan, "Redefining food safety traceability system through blockchain: Findings, challenges and open issues," *Multimedia Tools Appl.*, vol. 82, no. 14, pp. 21243–21277, Jun. 2023.
[69] G. Yang, T. Xiong, and H.-L. Ji, "Research on temperature control algorithm based on outlier mining in RFID," in *Proc. Int. Conf. Manage. e-Commerce e-Government*, Oct. 2012, pp. 275–279.
[70] G. Hendrik Haan, J. van Hillegersberg, E. de Jong, and K. Sikkel, "Adoption of wireless sensors in supply chains: A process view analysis of a pharmaceutical cold chain," *J. Theor. Appl. Electron. commerce Res.*, vol. 8, no. 2, pp. 21–22, 2013.
[71] M. Sivakumar and D. D. Deavours, "A dual-resonant microstrip antenna for paperboard in the cold chain," in *Proc. IEEE Sarnoff Symp.*, Apr. 2008, pp. 1–5.
[72] T. Mäkinen, "Parameter Configuration in Bluetooth Mesh: Performance and Limitations," M.S. thesis, Dept. Comput., Univ. Turku, Turku, Finland, 2025.
[73] M. M. Aung and Y. S. Chang, *Temperature Management in Cold Chain*. Cham, Switzerland: Springer, 2023, pp. 93–108.
[74] A. Coboi, M. T. Nguyen, V. N. Pham, T. C. Vu, M. D. Nguyen, and D. T. Nguyen, "Zigbee based mobile sensing for wireless sensor networks," *Comput. Netw. Commun.*, vol. 1, no. 2, pp. 325–342, Dec. 2023.
[75] S. S. Albouq, A. A. A. Sen, N. Almashf, M. Yamin, A. Alshanqiti, and N. M. Bahbouh, "A survey of interoperability challenges and solutions for dealing with them in IoT environment," *IEEE Access*, vol. 10, pp. 36416–36428, 2022.
[76] R. Jedermann, U. Praeger, and W. Lang, "Challenges and opportunities in remote monitoring of perishable products," *Food Packag. Shelf Life*, vol. 14, pp. 18–25, Dec. 2017.
[77] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "A comparative study of LPWAN technologies for large-scale IoT deployment," *ICT Exp.*, vol. 5, no. 1, pp. 1–7, Mar. 2019.
[78] R. Shafin, L. Liu, V. Chandrasekhar, H. Chen, J. Reed, and J. C. Zhang, "Artificial intelligence-enabled cellular networks: A critical path to beyond-5G and 6G," *IEEE Wireless Commun.*, vol. 27, no. 2, pp. 212–217, Apr. 2020.
[79] Z. Yin, Z. Wang, P. Liu, and Q. Shao, "Design and implementation of shipborne cold chain information collection system based on beidou short message," in *Proc. 5th Int. Conf. Electron. Commun., Netw. Comput. Technol. (ECNCT)*, Aug. 2023, pp. 299–303.
[80] U. Bhadani, "Comprehensive survey of threats, cyberattacks, and enhanced countermeasures in RFID technology," *Int. J. Innov. Res. Sci., Eng. Technol.*, vol. 11, no. 2, pp. 1803–1809, 2022.
[81] T. Ali, R. Baloch, M. Azeem, M. Farhan, S. Naseem, and B. Mohsin, "A systematic review of Bluetooth security threats, attacks & analysis," *Int. J. Comput. Trends Technol.*, vol. 69, no. 7, pp. 1–18, Jul. 2021.
[82] A. Zohourian, S. Dadkhah, E. C. P. Neto, H. Mahdikhani, P. K. Danso, H. Molyneaux, and A. A. Ghorbani, "IoT zigbee device security: A comprehensive review," *Internet Things*, vol. 22, Jul. 2023, Art. no. 100791.
[83] A. Kamilaris, A. Fonts, and F. X. Prenafeta-Boldú, "The rise of blockchain technology in agriculture and food supply chains," *Trends Food Sci. Technol.*, vol. 91, pp. 640–652, Sep. 2019.

FILIPPO GANDINO (Member, IEEE) received the M.S. and Ph.D. degrees in computer engineering from Politecnico di Torino, in 2005 and 2010, respectively. He is currently an Associate Professor with Dipartimento di Automatica e Informatica, Politecnico di Torino. His research interests include the IoT, security and privacy, complex systems, and information theory.

RENATO FERRERO (Senior Member, IEEE) received the M.S. degree in computer engineering and the Ph.D. degree in computer and system engineering from Politecnico di Torino, Italy, in 2004 and 2012, respectively. He is currently an Associate Professor with the Dipartimento di Automatica e Informatica, Politecnico di Torino. His research interests include ubiquitous computing, wireless sensor networks, and RFID systems, with applications in environmental monitoring and precision agriculture.