frontiers
in Sustainable Food Systems

ORIGINAL RESEARCH
published: 17 November 2020
doi: 10.3389/fsufs.2020.563424

Integrating Internet of Things, Provenance, and Blockchain to Enhance Trust in Last Mile Food Deliveries

Milan Markovic[1]*, *Naomi Jacobs*[2], *Konrad Dryja*[1], *Peter Edwards*[1] and
Norval J. C. Strachan[3]

[1] Department of Computing Science, University of Aberdeen, Aberdeen, United Kingdom, [2] Imagination Lancaster, Lancaster University, Lancaster, United Kingdom, [3] Department of Physics, University of Aberdeen, Aberdeen, United Kingdom

In this article, we discuss our experience of realizing a prototype IoT-based food safety monitoring solution which integrates inexpensive off-the-shelf open source IoT technology for monitoring food deliveries, semantic services for managing and reasoning about food safety provenance records, and private blockchain networks for persistent and secure storage of semantic provenance graphs. We describe how observation of real-world contexts was used to develop a prototype device, and the results of field trials deploying these prototypes as part of the food delivery process. Results indicate that continuous, context sensitive, trustworthy temperature measurement could provide benefits to multiple stakeholders across the delivery pathway. However, close attention has to be paid to the technology used—as cheap multi-functional IoT devices may produce low quality sensor observations which adversely affect the utility of the overall solution. Our experience also suggests that future food safety management systems may need to include machine-processable guidelines to support analysis of raw sensor data for food safety compliance.

Keywords: provenance, IoT, food safety, HACCP, blockchain, ontology

OPEN ACCESS

Edited by:
Andrea Zisman,
The Open University, United Kingdom

Reviewed by:
João Borges Laurindo,
Federal University of Santa Catarina,
Brazil
Marta Prado,
International Iberian Nanotechnology
Laboratory (INL), Portugal

****Correspondence:***
Milan Markovic
milan.markovic@abdn.ac.uk

Specialty section:
This article was submitted to
Sustainable Food Processing,
a section of the journal
Frontiers in Sustainable Food Systems

Received: *18 May 2020*
Accepted: *19 October 2020*
Published: *17 November 2020*

Citation:
Markovic M, Jacobs N, Dryja K,
Edwards P and Strachan NJC (2020)
Integrating Internet of Things,
Provenance, and Blockchain to
Enhance Trust in Last Mile Food
Deliveries.
Front. Sustain. Food Syst. 4:563424.
doi: 10.3389/fsufs.2020.563424

1. INTRODUCTION

In recent years, the advent of affordable Internet of Things (IoT) devices has enabled a number of novel data-driven innovations across many industries (Farooq et al., 2015). IoT sensing technologies offer inexpensive solutions for capturing and communicating observations about various aspects of real environments (e.g., air temperature) and interacting with physical and virtual objects (e.g., controlling a light switch, sending an email).

In the food industry, IoT is expected to become a key enabler for delivering enhancements to existing practices and to improve productivity (Kodan et al., 2019). However, the use of IoT in food safety, such as temperature monitoring of perishable foods is still a relatively niche area with the majority of research being conducted in China and very few research studies applied to the European context (Bouzembrak et al., 2019). We argue that monitoring of this type is especially important in those segments of the food supply chain that involve different people and businesses responsible for food handling (we refer to them as agents) and changing physical locations, such as the food delivery process, particularly in contexts where this may also involve diverse modes of transport (e.g., cars, vans, bicycles, walking, etc.). Food chains can be complex and a number of stages are involved in a typical delivery chain, during which an order is first made available for delivery, then collected by a delivery person, stored in a vehicle, and transported to the customer. As highlighted in the UK Food Standards Agency strategic plan 2015–2020[1] and enshrined in the law: "It is the responsibility of businesses producing and supplying food to ensure it is safe and what it says it is . . . ." Many businesses today address this through a series of manual tasks (e.g., temperature checks of perishable items using manual probes) and paper based record keeping following the procedures defined in their HACCP food safety management systems (Mortimore and Wallace, 2013). Such systems consist of three components: (awareness of) hazards, control measures, and critical control points. Hazards are anything that may introduce harm to customers, and may include microbiological, chemical or physical agents. Control measures are ways to prevent or control these hazards. Critical control points are stages where control can be applied to prevent or reduce a food safety hazard to an acceptable level. For example, for chilled food to be considered safely stored, normally the temperature must be no higher than 5°C to eliminate microbiological growth (the hazard) (Food Standards Agency, 2016). 5°C is therefore the "critical limit." There is a clear opportunity for automation of temperature measurements and other environmental sensing through IoT at various critical control points (e.g., while food is stored in a fridge) defined in HACCP plans (Tian, 2017).

IoT technologies offer several benefits in comparison to the traditional methods used for monitoring such critical control points and limits. IoT devices can be battery operated and small in size and thus can be easily packed together with food, while also being capable of recording a variety of environmental qualities including temperature (an important factor in food safety management). In comparison with traditional temperature loggers, IoT devices may offer a wider range of connectivity options (e.g., Bluetooth, LoRaWAN, WI-FI, GSM, etc.) and may also possess greater on-board processing power. This enables computations to be performed by the IoT device itself, enabling them to act as location and context aware devices that document and react to changes in their physical surroundings; they may also aggregate data and perform inferences. However, we argue that to integrate such devices into a food supply chain and to derive meaningful conclusions about the safety of food products more contextual information is needed to enable correct interpretation of raw sensor data and alerts produced by IoT devices. To describe the full delivery process, such information has to be linked into a coherent story describing the journey of the delivered food item through the individual steps of a delivery workflow. Capturing such information requires appropriate data models capable of contextualizing measurements and documenting how they were processed; this means capturing *what*, *how*, *when*, *why*, by *whom*, and *where* data were collected, and *which* conclusions were drawn from the observations.

Here, the existing standard in provenance modeling PROV (Moreau and Groth, 2013) provides a useful core data model for describing such metadata. The W3C PROV recommendation defines provenance as records describing "the people, institutions, entities, and activities involved in producing, influencing, or delivering a piece of data or a thing" (Moreau et al., 2015). In our previous research, we demonstrated that a PROV-based approach can be successfully applied to capture the journey of a food item through the different stages of a food preparation workflow in a commercial kitchen setting (Markovic et al., 2016). We argue that a similar approach could be applied to the food delivery domain, which would encompass firstly capturing what is expected to happen during the delivery process (i.e., a delivery plan) so it can be later linked with the provenance of the actual delivery process (i.e., describing what really happened during the delivery).

However, the utility of such information can only be realized if it is trusted and available, which is a non-trivial challenge in a heterogeneous, multi-stakeholder environment, such as the food industry. Recently, Distributed Ledger Technologies (DLT), such as blockchain, and smart contracts have emerged as a promising approach to facilitate permissioned, transparent, and secure exchange of immutable data records between members of business blockchain networks (Reyna et al., 2018). Blockchain has been gaining attention from both research communities and industry due to its potential to enhance the traceability of food items in the food supply chain (Pearson et al., 2019). In this context, provenance information recorded from heterogeneous sources (sensors, human input, document scanning, etc.) is often cited as one of the important pieces of metadata that supports traceability and food safety assessments. Data produced by IoT-based monitoring of different food supply stages, such as harvesting, processing, wholesale distribution, and retailing in combination with blockchains is expected to be a key enabler in producing robust and trustworthy solutions for food traceability (Tian, 2017; Pal and Kant, 2019). However, many challenges, such as those relating to scalability, data collection and integration, and standardization need to be solved before DLT can be adopted industry-wide (Pal and Kant, 2019; Pearson et al., 2019). We argue that combination of other existing technologies and DLT will be required to address these challenges. For example, semantic technologies, such as ontologies (OWL Working Group, 2012) and linked data (Bizer et al., 2011) may help address the standardization and data integration challenges currently faced by food businesses and regulators. Such technologies can produce machine-understandable knowledge graphs and have been previously recognized for their benefits in the context of knowledge representation, information interoperability, integration and linking as part of decision support systems (Blomqvist, 2014).

This article describes our recent efforts to assess feasibility and practicality of combining open source IoT devices, semantic technologies, and DLT for food safety compliance monitoring in a real world setting. The research described here was framed by the following research questions:

- Can IoT devices be used to monitor compliance of food deliveries with temperature constraints defined by HACCP food safety management systems?

[1] https://www.food.gov.uk/sites/default/files/media/document/FSA-Strategic-plan-2015-2020.pdf

- Can IoT devices be used to transform raw sensor observations into concise compliance records which can then be represented as machine-understandable knowledge graphs?
- Is it possible to store and share compliance provenance reports using DLT?
- How do customers and business operators perceive the utility of an IoT-based food safety monitoring system?

These questions were investigated through development and deployment of a prototype IoT-based food safety monitoring system called PROoFD-IT (PROvenance of Food Delivery through IoT). In this article, we report the results of two system deployments in real food delivery settings, followed by a series of quantitative evaluations of systems performance as well as qualitative studies involving business operators and customers.

The remainder of the paper is structured as follows: section 2 summarizes a selection of related work across several topics including IoT, provenance, food safety monitoring and blockchains; section 3 details our approach including the journey mapping exercise conducted in partnership with our project business partners and the application scenario which drove the design of the PROoFD-IT system; sections 4, 6, and 7 detail the design and implementation of the PROoFD-IT system as well as two rounds of system evaluation in real food delivery settings; sections 8 and 9 conclude the article with discussion and plans for future work.

2. RELATED WORK

2.1. Food Safety Monitoring and IoT

A number of solutions have been proposed where IoT technology is used to monitor food safety and control food quality using environmental sensing and smart product tags (Bouzembrak et al., 2019). Some of the proposed solutions utilize temperature measurements and locations provided by IoT devices to monitor the cold chain containing products, such as meat, shellfish, fruit, and vegetables. For example, Tian (2017), proposes a HACCP based food supply traceability system incorporating sensor readings to monitor various aspects of food products across different supply stages, such as temperature, humidity, product quantity, storage time, etc. However, the concept was not tested via a prototype implementation. Chen et al. (2014) propose a new approach to managing smart cold chain systems based on novel RFID technology. The passive tags carry an executable code (unique to a specific food product) containing expected storage conditions which is then interpreted by the middleware against the current environmental readings (e.g., from IoT temperature sensors). Shih and Wang (2016) propose a wireless temperature monitoring system based on critical control point criteria covering the various stages of a multi-channel Chinese food processing system. Tsang et al. (2018) proposed an IoT based intelligent route planning model for food deliveries that utilizes live IoT data (such as temperature and humidity readings) to optimize delivery routes in order to ensure the quality of different types of fruits and vegetables.

One of the challenges for IoT technologies in the food safety context is the need to deliver sensing of acceptable quality for compliance checking. In the UK, food safety compliance is routinely evaluated through manual inspections by environmental health officers who follow specific protocols when monitoring temperature. We argue that businesses utilizing IoT should adhere to very similar monitoring standards in order to prevent issues during inspections. For example, the Food Law Practice Guidance (England) (Food Standards Agency, 2017) provides guidance on temperature checks and equipment used for enforcement of Regulation 32/Schedule 4 of the Food Safety and Hygiene (England) Regulations 2013.[2] The guidance lists three stages of temperature control namely air temperature monitoring (to check the air temperature maintained by the refrigeration system); between-pack testing (non-destructive surface temperature testing of individual food items with additional 2°C tolerance); and product testing (destructive temperature testing by piercing the product with a probe).

The guidelines further state that temperature measurements taken for the purposes of enforcement should not be prejudiced by events, such as opening of refrigerator doors, or removing the food from a chilled environment for long periods before testing. The equipment must also meet a number of requirements: it must be subject to regular (re)calibration; it must deliver accuracy of at least ±0.5°C (with a maximum allowed deviation of ±0.3°C in the −20 to +30°C range); it must be robust and shock proof; and it must reach 90% of the final reading within 3 min. These requirements, in particular the accuracy and speed of measurement, may prove challenging for many of the low-cost IoT sensors available on the market today—limiting their potential use for compliance monitoring. Furthermore, we believe that these issues are not sufficiently considered by the existing literature, and temperature readings provided by these technologies are too often taken at face value. For example, the DS18B20[3] temperature probe (reported accuracy ±0.5°C and also used in our project) has been used in other food related research due to its low cost; examples include monitoring of refrigeration units (Ramírez-Faz et al., 2020), and freshwater aquaculture production (Shi et al., 2018). However, authors did not report any calibration or evaluation of sensor accuracy and the temperature readings seem to be taken at their face value.

2.2. Provenance, Ontologies, and The Digital Food Chain

In recent years, traceability in food chains has become a widely discussed topic following high profile events, such as the UK horse meat scandal (Department for Environment, 2013). New (2010) describes how consumers, governments and organizations demand information on various aspects of supply chains (e.g., location and origin of products) across diverse industry sectors, and argues that technologies, such as IoT can facilitate recording of fine grained provenance information about individual items moving through different parts of the supply chain.

[2] http://www.legislation.gov.uk/uksi/2013/2996/contents/made
[3] https://datasheets.maximintegrated.com/en/ds/DS18B20.pdf

Provenance data models record contextual information about agents, activities and entities, which provide answers to *what*, *where*, *when*, *how*, *who*, *which*, and *why* questions (Ram and Liu, 2009). In digital food chains, provenance may be understood as a causal graph of events/activities (food processing steps) detailing all individual agents responsible for them (food processing businesses, customers) and the entities (food items) used and produced during these activities. For this reason, provenance records are retrospective and are generated after the events have occurred. Such records may then support various auditing processes, such as traceability of food items (Batlajery et al., 2018).

Semantic ontologies define formal models expressed using standard machine-processable languages to explicitly describe concepts and their semantic relationships for a specific domain (OWL Working Group, 2012).

Ontologies can be described using the OWL 2 language—a W3C[4] recommendation. For a specific domain, an ontology defines the types of concepts (i.e., classes) that can be described (e.g., a *Fresh Meat Item*, *Delivery Process*) and relationships (i.e., properties) between these concepts (e.g., a Fresh Meat Item may be *part of* a delivery process). Concrete or abstract objects that belong to a class defined in an ontology are described as individuals. For example, an individual describing a specific food item (e.g., a chicken breast pack) may be associated with the *Fresh Meat Item* class to express its type (i.e., the chicken breast pack is a member of the *Fresh Meat Item* class). Individuals then may be linked to other individuals or literals (i.e., plain text, date, numbers, etc.) using object and data properties to produce semantic graphs. For example, an individual belonging to the class *Fresh Meat Item* may be linked using the object property *part of* to an individual belonging to the class *Delivery Process* to describe that this item was delivered. The individual of the type *Delivery Process* may then be further described using data properties, such as *has delivery date* which link the individual to corresponding literal values. The semantic graphs are described using the Resource Description Framework (RDF) (Patel-Schneider and Hayes, 2014) which captures data in the form of triples, where each triple has three parts: *subject*, *predicate*, and *object*. Each part of a triple is associated with an internationalized resource identifier (IRI)[5]. For example, **Figure 1** (left) illustrates part of a semantic graph describing various information about a sandwich delivery uniquely defined as an individual *Delivery123*. Three statements (triples) associate the *Delivery123* with a type *prov:Activity*, a human readable text description, and the item used in the delivery defined as *Sandwich1*.

Such graphs may be queried using the SPARQL query language (Harris and Seaborne, 2013). SPARQL queries return instances that match user-defined query patterns. For example, the simple SPARQL query shown in **Figure 1** (right) would return all individuals of type *prov:Activity* that *prov:used* a specific entity *Sandwich1* (i.e., in this case the process *Delivery123*).

In recent years, semantic web technologies (such as ontologies, linked data, graph storage solutions, etc.) were proposed in the context of e-Government (Klischewski, 2015) and Open Government Data (Charalabidis et al., 2016) as potential means to deal with data standardization and data aggregation from multiple entities (e.g., councils, transport providers, etc.). We argue that such technologies, in combination with standard provenance models, have the potential to support food industry scenarios that require data integration from heterogeneous data sources (e.g., food businesses, councils, customers) using standard vocabularies; for example, as part of a compliance monitoring platform for food regulators.

The W3C recommendation PROV-O (Lebo et al., 2013) is a general purpose ontology for representing provenance. PROV-O was the result of a comprehensive design process building on previous provenance work from the database and workflow communities. It supersedes previous provenance models, such as the Open Provenance Model (OPM) (Moreau et al., 2011) and various mappings to other standards, such as the Dublin Core (Eckert and Garijo, 2013) already exist; for more details on the design rationale of PROV-O (see Moreau et al., 2015). Semantic provenance graphs may be further enriched by links to other information described using other ontologies. For example, the Semantic Sensor Network ontology (Haller et al., 2017) can be used to describe sensor observations, details of the sensors producing the observations, and their deployment setting. We have previously demonstrated how PROV-O can be extended in order to document the individual steps and constraints associated with HACCP-based workflows (Markovic et al., 2016). The resulting FS-PROV ontology forms part of the solution discussed in this paper, and is further described in section 4.4.

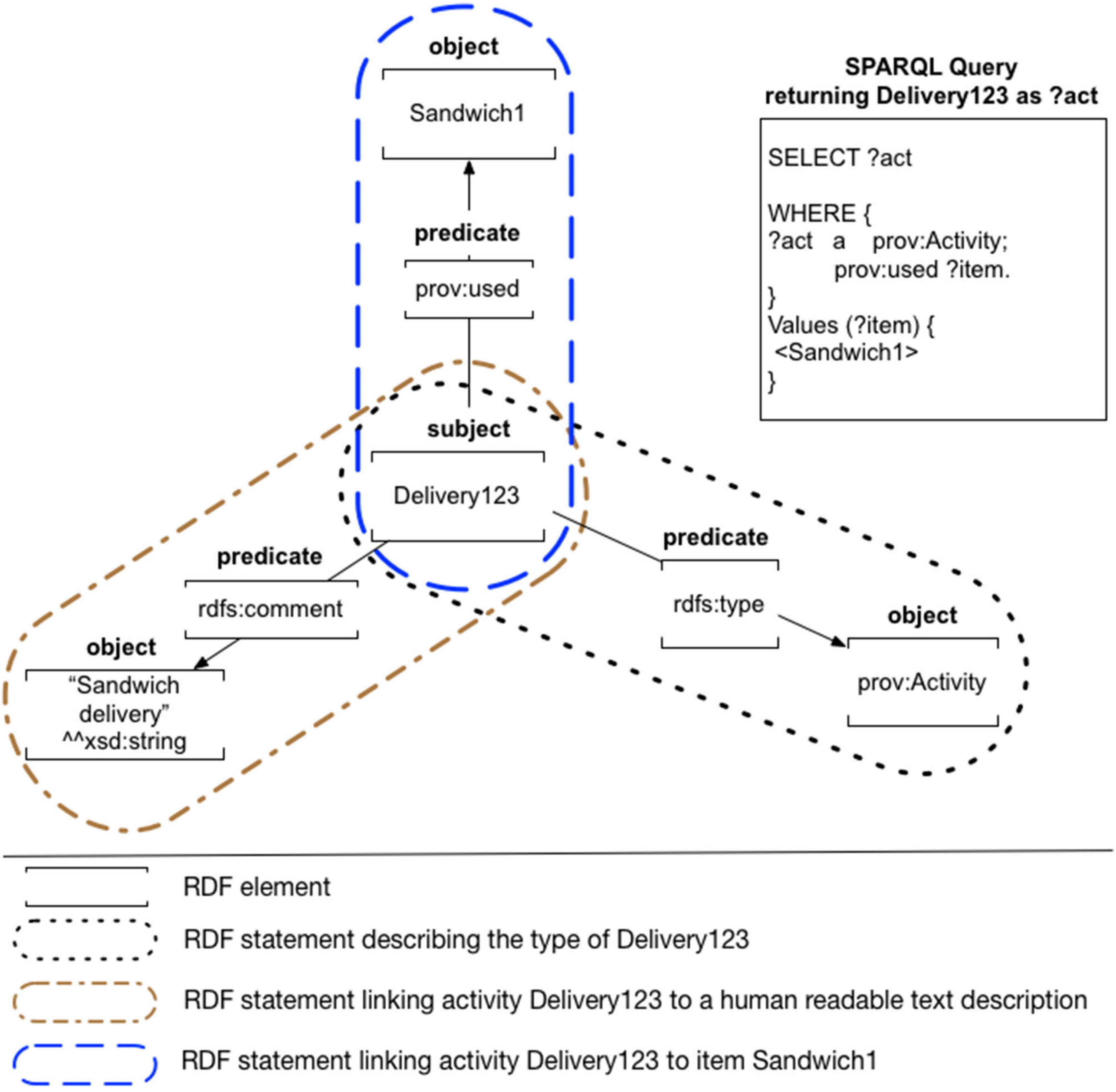
2.3. Blockchain in the Food Sector

Distributed ledger technologies (DLT) have been designed to provide an immutable, transparent, and trusted storage solution which distributes the stored information across many independently owned nodes and hence increases protection against data corruption and malicious modification (Nærland et al., 2017). Blockchain is a type of DLT that provides immutable trusted data storage of events/transactions based on cryptographic proofs and was initially popularized by the online crypto currency market (Nakamoto, 2019). Blockchain networks can support "smart contracts" which are programs that can execute on the network and define, for example, the structure of transactions that business can complete on the network (e.g., to purchase and sell assets as they are moving through a supply chain) (Nærland et al., 2017).

In the food industry, blockchain networks have been proposed to support novel applications for traceability, agricultural insurance, forestry economics and prevention of illegal and unsustainable fishing (Caro et al., 2018; Kamilaris et al., 2019; Sylvester, 2019). Blockchain-based solutions offer potential

[4] World Wide Web Consortium; https://www.w3.org/TR/owl2-overview/

[5] A prefix separated by : abstracts the repetitive parts of the IRI.


object
Sandwich1
predicate
prov:used
subject
Delivery123
predicate
rdfs:comment
object
"Sandwich delivery" ^^xsd:string
predicate
rdfs:type
object
prov:Activity
SPARQL Query returning Delivery123 as ?act
RDF element
RDF statement describing the type of Delivery123
RDF statement linking activity Delivery123 to a human readable text description
RDF statement linking activity Delivery123 to item Sandwich1

```
SELECT ?act

WHERE {
?act  a   prov:Activity;
       prov:used ?item.
}
Values (?item) {
 <Sandwich1>
}
```

FIGURE 1 | An overview of semantic technologies for representing and querying graph data.

benefits in food safety, food security, food integrity and waste management (Kamilaris et al., 2019). Systems utilizing both IoT devices and blockchains have been proposed to enhance food logistics (Pal and Kant, 2019) and food safety in food supply chains (Tian, 2017). While some mature platforms already exist (e.g., Food Trust from IBM[6]) other blockchain systems in the food sector are still in their early stages of implementation, either proposed as theoretical systems or deployed as pilot studies focusing on specific aspects of the food supply.

3. METHODOLOGY AND APPLICATION DOMAIN OVERVIEW

In this project we have brought together an interdisciplinary team of researchers contributing their expertise from fields of computer science, design and food sciences. Design methodologies including user journey mapping (Schneider and Stickdorn, 2011) were used to develop use case scenarios that drove the requirements engineering process for the aforementioned prototype IoT-based food safety monitoring system called PROoFD-IT. The design went through an iterative

[6] https://www.ibm.com/uk-en/blockchain/solutions/food-trust

process following the feedback from intermediary user trials in real world settings. The design solution was evaluated using a mixed-methods approach using both qualitative methods, such as interviews and qualitative surveys[7], and quantitative techniques which evaluated the accuracy of temperature measurements produced by low-cost IoT devices by benchmarking these against observations produced by a certified sensor. In this way, it was possible to assess the technical and practical feasibility of such a solution in real-world deployments.

3.1. Food Delivery Journey Mapping

The initial stage in the development of the prototype was to understand the context in which it would be deployed including the human actors who function as part of the food delivery process; producers and consumers. We worked with two commercial partners who acted as case studies in real-world examples of the delivery of chilled food. The first of these partners is a meat production and delivery company called G. McWilliam Aberdeen Ltd.,[8] who process a range of meat products and deliver to businesses across the region including restaurants, schools, and hospitals. Food is prepared, stored and delivered in a chilled environment, the latter via temperature controlled vans. The second partner was the University of Aberdeen Catering Service who provide a range of ready-to-eat food to staff and external customers on the university campus. This includes both hot and cold food which is intended for immediate consumption.

Through observation documented by photo-mapping, alongside interviews with business representatives, the full delivery process was examined which allowed us to construct journey maps for deliveries undertaken for each of the two partners. **Figure 2** shows an abstracted exemplar journey map. In order to preserve privacy and abide by ethical research practices, the map displayed does not specify the full process examined in either of the case studies, but instead includes representative stages illustrating the complex nature of a typical delivery process.

Key observations from this process included the following:

- Each journey includes a number of key points at which food is transferred between areas of different standard temperatures. These are points at which there is potential for safety risk through a rise in temperature, particularly if unforeseen circumstances arise or policies are not abided by, and especially if this includes transfer between different individuals or organizations.
- In the current delivery processes, temperature checks are carried out at key points to ensure food safety compliance. The intermittent nature of these readings means that they record temperature at a specific point but provide limited information about temperature changes which may have occurred during the time since the last reading. There is the opportunity to gain further insights via constant temperature monitoring, which may be of use to businesses and customers.
- The frequency and method of implementing and recording temperature checks can vary depending on the context, and the requirements of particular stakeholders. Currently, temperature readings are primarily recorded manually via paper records.

These observations informed the application scenario for the PROoFD-IT system, which was designed to enhance current food safety monitoring practices implemented by businesses by introducing continuous temperature monitoring of food items throughout the delivery process, increasing the availability of food safety data, and reducing the need for paper-based record keeping.

3.2. PROoFD-IT System Application Scenario

In this section, we introduce our application scenario which was used to drive the design and evaluation of the PROoFD-IT computational framework.

The system starts monitoring the food items from the point when the items are packed and prepared for delivery. At this stage, a reusable IoT device is associated with the delivery package (by attaching it to the lid of the delivery box) and begins monitoring the air temperature around the food items. The IoT monitor is pre-programmed with a device ID and the ID of the delivery order which is being monitored. The delivery ID is used to identify and link the provenance record produced by the device to specific deliveries. The IoT monitor stays attached to the delivery package until it reaches the customer. This process usually involves several steps in the delivery workflow, such as cold storage, pick up by the delivery person, storage in the delivery vehicle, and finally handover to the customer, who decides whether to accept or reject the delivery. The IoT monitor identifies its current location by scanning for IoT beacons that are positioned in fixed locations (e.g., in a cold storage unit, or delivery vehicle). Based on its current location, the device computes whether any of the food safety constraints relevant for that stage of the delivery workflow have been breached. For example, a breach is detected if a food item has been left outside refrigerated storage for a significant amount of time. A summary report detailing the overall delivery process as well as more detailed compliance information for each of the individual steps is communicated to the user via a mobile app interface. The same information is then also stored as a semantic graph on an immutable blockchain network. Such data can then be accessed for audit purposes or integrated with other datasets and applications by third party entities that have been granted data access privileges.

4. PROoFD-IT SYSTEM OVERVIEW

The PROoFD-IT system was developed to deliver the functionality of smart food safety compliance monitoring using IoT, blockchains, and semantic provenance capture mechanisms. The remainder of this section describes the overall design of the system, and the implementation of its individual components; we also discuss current system limitations, and

[7] These studies were approved by the University of Aberdeen's Physical Sciences and Engineering ethics board.

[8] https://www.gmcwilliam.co.uk

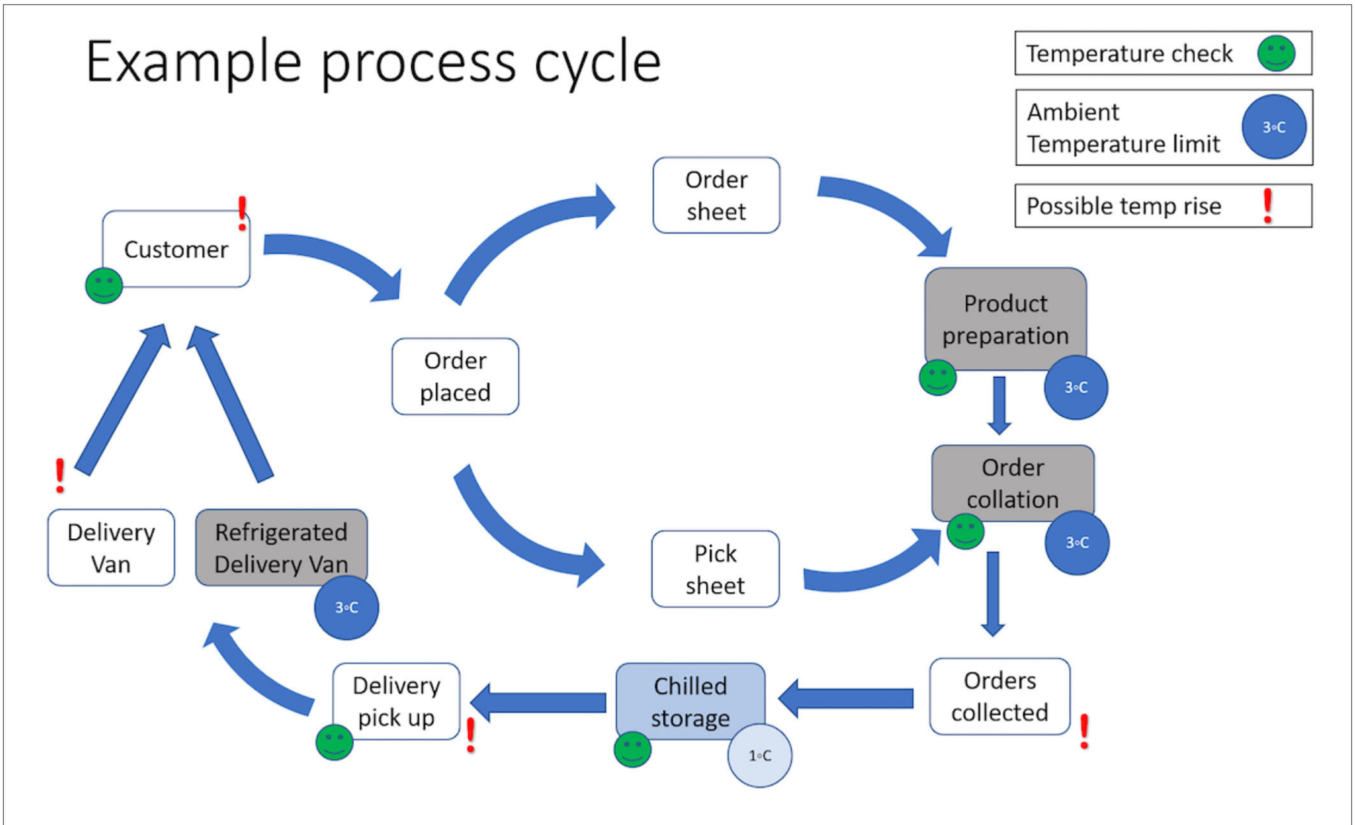


FIGURE 2 | An overview of the main delivery steps derived from on-site observations with project business partners.

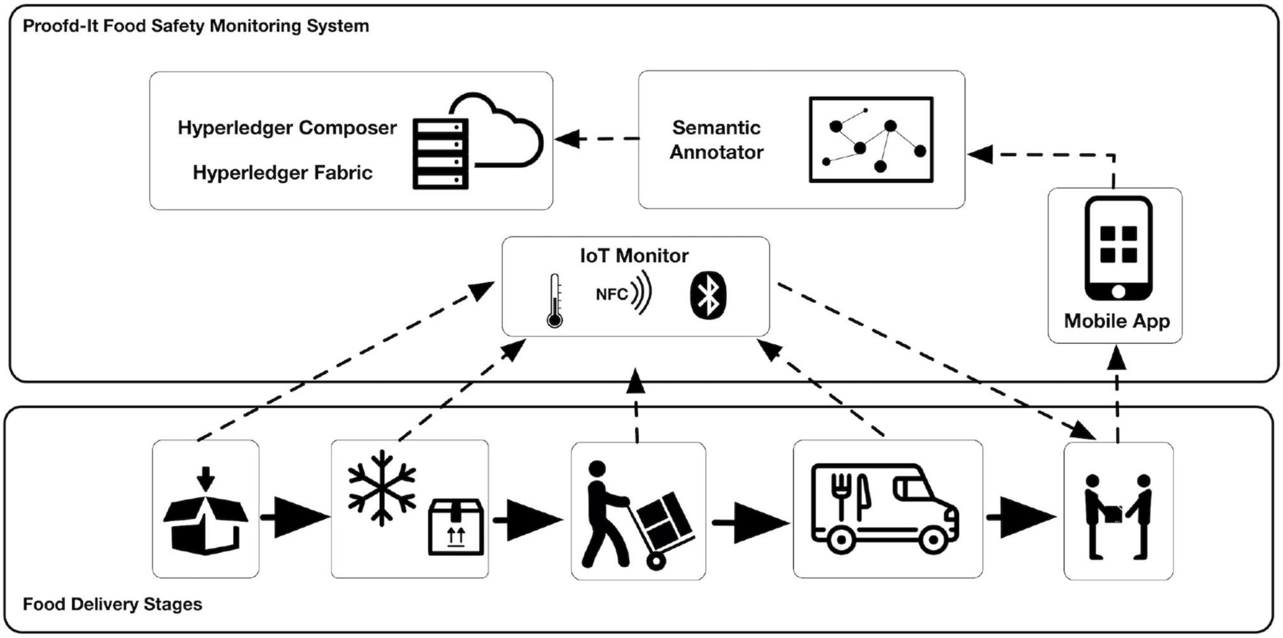


FIGURE 3 | A high level overview of the main components within the PROoFD-IT food safety monitoring system.

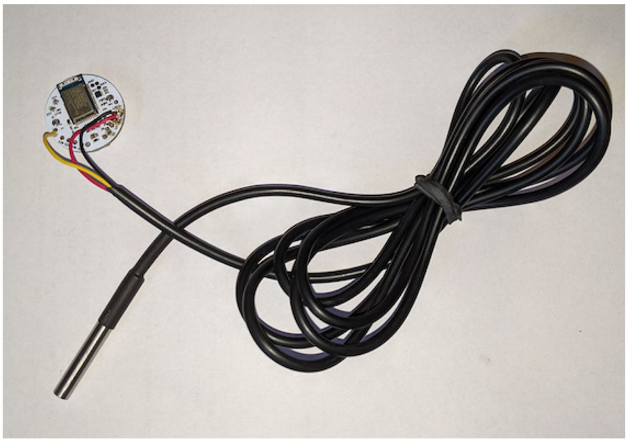


FIGURE 4 | The IoT monitor consisting of the Puck.js device with attached DS18B20 temperature probe.

provide a summary of lessons learnt relating to the accuracy and quality of the IoT devices used.

4.1. Architecture

The system architecture consists of four main components shown in **Figure 3**: IoT monitors and location beacons; a mobile application for users to interact with the compliance monitoring data; a server application for generating semantic annotations; and a blockchain network for persistent storage. The system is designed to identify different delivery stages, such as cold storage, transport, and out of temperature control stage. The IoT monitor and location beacons are implemented using Puck.js[9] (an open source Espruino[10] based device), the mobile app is implemented as a simple progressive Web app (i.e., it does not require installation on the device), the semantic annotator is implemented as a JAVA Spring Boot[11] server application, and the blockchain network is implemented using the Hyperledger Composer[12] wrapper utilizing the Hyperledger Fabric[13] layer.

4.2. Intelligent IoT Monitor

Puck.js (**Figure 4**) is a multi-purpose Epsruino-based IoT device capable of performing simple computational operations and comes pre-installed with a range of built-in sensors for detecting light, magnetic fields, physical button presses, and temperature. The device can interact with the outside environment through LEDs, Bluetooth, and NFC. Epsruino is described as JavaScript for micro-controllers, allowing initial development of all instructions in JavaScript. To increase the precision and accuracy of the temperature readings, an external temperature probe (DS18B20) was attached to the device (for more details and rationale see section 5).

The IoT monitor software is available through GITHUB[14] and includes two main program loops that run constantly until a button press event is observed (i.e., to mark the end of the delivery process by the customer). The first loop is responsible for periodically scanning for nearby Bluetooth beacons (also implemented using Puck.js devices) to determine whether the location has changed. Typically, the device recognizes three locations which correlate to the typical stages of a food delivery workflow: *fridge*, *transport*, and *outside* which is a default option if no location beacons are detected. The second loop is continuously checking for temperature[15] using the attached probe. If a constraint encoding a maximum allowed temperature for a specific delivery stage has been exceeded (e.g., a HACCP threshold for cold storage), the device will enter "alert" mode and increases the measurement frequency. If four consecutive readings[16] exceed this threshold, an event is logged to mark the current delivery stage as non-compliant and readings demonstrating this non-compliance are also stored. If the readings corresponding to a specific workflow stage do not breach any constraints, none of the detailed sensor readings are stored.

Below, we list all currently defined timings and constraints to illustrate the monitoring features supported by the IoT device. Please note that the values for the constraints were specified to support monitoring of specific delivery workflows during our trials, and different values may be required for other use cases.

- Scanning for location beacons is performed every 7 min and then again after 1 min if a different location/stage is detected. Each scan lasts for 2.5 s.
- Temperature measurement frequencies:
    - ⋆ *Outside*—every 10 min
    - ⋆ *Transport*—every 15 min
    - ⋆ *Fridge*—every 20 min
    - ⋆ *Alert Mode (applies to all stages)*—every 7 min
- Temperature constraints:
    - ⋆ *Outside*—$< 25°$C
    - ⋆ *Transport* and *Fridge*—$< 5°$C
- Temporal constraints restricting maximum duration of individual stages:
    - ⋆ *Outside*—allowed to occur once and no longer than for 3 h
    - ⋆ *Transport*—no longer than 3 h in total
    - ⋆ *Fridge*—no longer than 48 h in total

At the end of the delivery process, the data produced by the IoT monitor containing a list of observed delivery stages and details of any temperature and temporal constraint breaches are

[9] https://www.puck-js.com/

[10] https://www.espruino.com/

[11] https://spring.io/projects/spring-boot

[12] https://hyperledger.github.io/composer/latest/

[13] https://www.hyperledger.org/projects/fabric

[14] https://github.com/PROoFD-IT/IoT-monitor

[15] The frequency of scans depends on the current location, i.e., in the fridge the scans are performed less often than if the device is located outside.

[16] A grace period of three-consecutive-readings have been included to rule out false-positives resulting from temperature changes caused by fridge compressor cycles or by increased usage of the fridge (i.e., the door is opened, temporarily warming the temperature inside).

parsed into JSON.[17] The JSON payload is then communicated via Bluetooth to a mobile app operated by the client receiving the goods.

4.3. Mobile App

The mobile application is a simple progressive Web-based app developed using HTML and JavaScript. It utilizes the Web Bluetooth API[18] to download data from IoT monitors. The app is hosted as a Web page on an online server with HTTPS address encoded to the IoT monitor's NFC tag (e.g., https://example.com/app?n=e4b3074). When the NFC tag is read by a phone, the phone automatically displays the mobile app and initiates a Bluetooth pairing process between the phone and the IoT device.

Figure 5 illustrates three mobile app screenshots visualizing data recorded by the IoT monitor. In this case, two delivery stages stages (*Fridge* and *Outside*) were recorded during the delivery process. Each stage is associated with an assessment result indicating whether any anomalies were detected during that stage. Each description can be expanded (**Figures 5B,C**) to display additional information. If a stage is assessed as non-compliant with the encoded temperature constraints (**Figure 5B**) a collection of sample readings that have breached the temperature threshold is displayed for user consideration. This is to enable users to consider the assessments of borderline cases (e.g., four readings 0.8°C above the threshold may be still acceptable under certain scenarios). However, if the stage was assessed as compliant only a summary text explaining the evaluation constraint is displayed as the IoT monitor does not store any readings that are below the required thresholds (**Figure 5C**). After pressing accept/reject buttons, the information received from the IoT monitor is amended with the record of acceptance/rejection of the delivery and forwarded to the cloud infrastructure.

4.4. Server Application

The server application receives a JSON object containing the data generated by the IoT monitor and forwarded by the mobile app. The data are parsed and semantically annotated using ontologies and Apache JENA Java library[19] to generate food safety compliance records which are then stored on the blockchain network. In our system, the food safety data is described using several pre-existing ontologies namely W3C PROV-O (Lebo et al., 2013), FS-PROV (Markovic et al., 2016), EP-PLAN (Markovic et al., 2019), the SOSA ontology [a core part of the W3C Semantic Sensor Network Ontology (SSN)] (Haller et al., 2017) and the PROoFD-IT ontology (a domain extension of PROV-O defining several utility concepts and relations).

The compliance record is described as a provenance graph consisting of three main components (as shown in **Figure 6**):

- *Plan*: Specification of the delivery plan defining the steps that a delivery process was expected to follow and associated constraints at both plan and step level (e.g., required temperature levels for steps denoting cold storage, maximum allowed combined duration for all cold storage steps in the plan, etc.).
- *Execution Trace*: Record of the different stages of the delivery process as they occurred, including records of constraint compliance and violation. This is recorded as a detailed execution trace with corresponding links to relevant parts of the plan.
- *IoT Sensing Provenance*: Record of additional contextual information detailing how the temperature observations were generated and constraints evaluated.

The W3C PROV-O recommendation (Lebo et al., 2013) utilizes three core concepts to describe provenance namely, *entities*, *activities*, and *agents*. *Entities* represent any physical or virtual assets that can be manipulated by *activities* (e.g., used and produced) for which *agents* assume some form of responsibility. PROV provides a suitable base model for modeling execution traces (i.e., record of what happened), however, only a high level generic concept of plans is defined (Moreau et al., 2015). However, in our research context it is important to have more detailed descriptions of the plan in order to provide the ability to discover deviations between the expected and the actual execution of the delivery process.

4.4.1. Modeling Plans and Corresponding Execution Traces

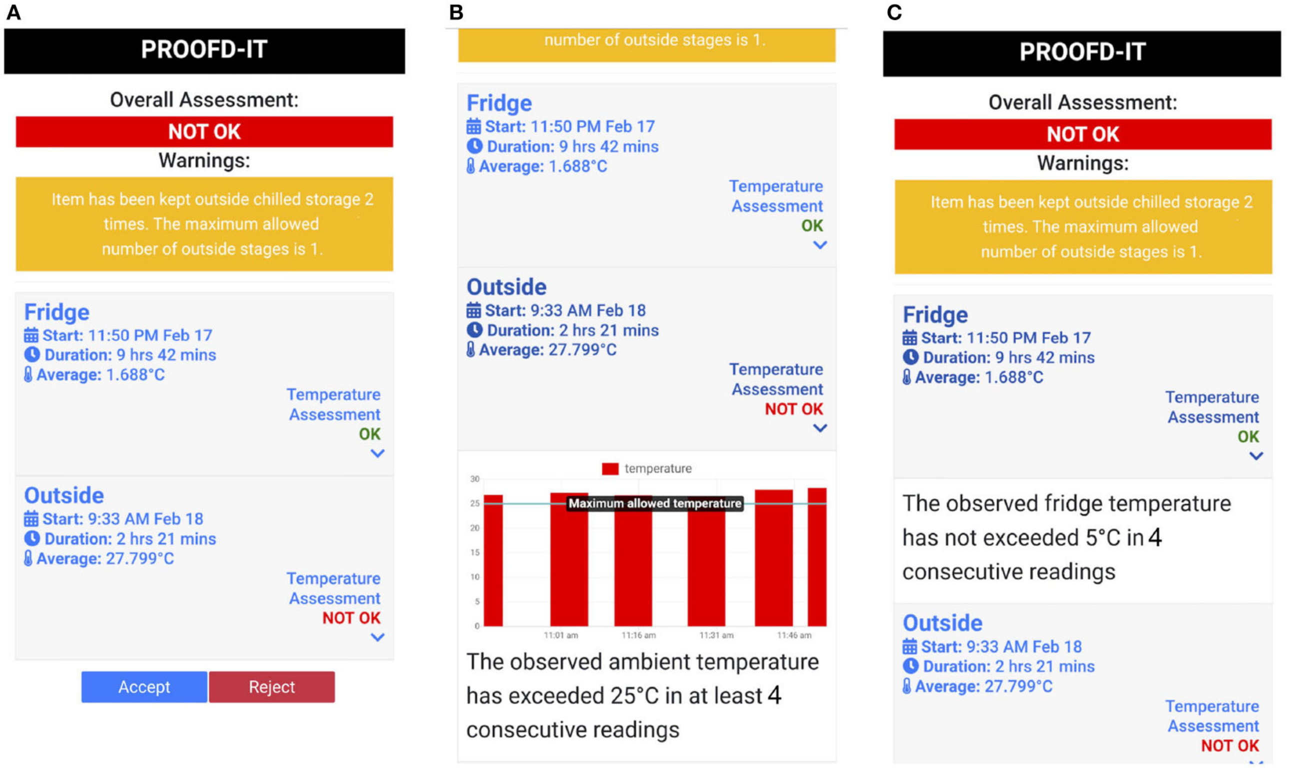
To provide more detailed descriptions of the delivery plans we used the EP-PLAN ontology (Markovic et al., 2019). EP-PLAN extends PROV-O to enable descriptions of plans as acyclic graphs where nodes represent individual elements of a plan specification, such as steps, variables, and constraints. In EP-PLAN, steps represent individual planned processes and are connected with other steps via the input and output variables representing data or real objects that such processes use and produce. Steps and whole plans may be associated with descriptions of constraints (e.g., to restrict the type of inputs used, location where the processes should be executed, etc.).

In EP-PLAN, plan descriptions may be linked to provenance descriptions documenting actual plan execution. For example, **Figure 7** illustrates an example *Meat Delivery Plan* and the four high level constraints associated with that plan, namely *total time allowed for cold storage*, *total time allowed for transport*, *total time allowed for ambient temperature storage*, and *total number of allowed ambient temperature storage stages*. Since EP-PLAN is a generic model aimed at cross domain applications, to specialize the individual steps, variables, and constraints, we use classes defined as part of the FS-PROV ontology which uses a similar underlining model to describe detailed plans. FS-PROV has been designed to include more specific classes denoting physical objects, HACCP steps and HACCP constraints to describe provenance in the food related context. **Figure 7** also illustrates the capture of the high level delivery process (*Meat Delivery*) modeled as a *ep-plan:Activity*. This activity is linked to *ep-plan:Agent* (*Food Delivery Business*) denoting the business entity responsible for making the deliveries. The delivery activity is also linked to the aforementioned plan constraints (e.g.,

[17] https://www.json.org/json-en.html

[18] https://developer.mozilla.org/en-US/docs/Web/API/Web_Bluetooth_API

[19] https://jena.apache.org/



PROOFD-IT

Overall Assessment:

NOT OK

Warnings:

Item has been kept outside chilled storage 2 times. The maximum allowed number of outside stages is 1.

Fridge
Start: 11:50 PM Feb 17
Duration: 9 hrs 42 mins
Average: 1.688°C
Temperature Assessment OK

Outside
Start: 9:33 AM Feb 18
Duration: 2 hrs 21 mins
Average: 27.799°C
Temperature Assessment NOT OK

Accept | Reject

number of outside stages is 1.

Fridge
Start: 11:50 PM Feb 17
Duration: 9 hrs 42 mins
Average: 1.688°C
Temperature Assessment OK

Outside
Start: 9:33 AM Feb 18
Duration: 2 hrs 21 mins
Average: 27.799°C
Temperature Assessment NOT OK

The observed ambient temperature has exceeded 25°C in at least 4 consecutive readings

PROOFD-IT

Overall Assessment:

NOT OK

Warnings:

Item has been kept outside chilled storage 2 times. The maximum allowed number of outside stages is 1.

Fridge
Start: 11:50 PM Feb 17
Duration: 9 hrs 42 mins
Average: 1.688°C
Temperature Assessment OK

The observed fridge temperature has not exceeded 5°C in 4 consecutive readings

Outside
Start: 9:33 AM Feb 18
Duration: 2 hrs 21 mins
Average: 27.799°C
Temperature Assessment NOT OK

FIGURE 5 | Mobile app screenshots displaying two delivery stages recorded by the IoT monitor. Screenshot **(A)** shows a high-level overview of the compliance report; screenshot **(B)** shows an expanded view of a non-compliant stage with sample temperature readings that violated the temperature threshold; screenshot **(C)** shows an expanded view of compliant stage with a summary explanation.

Total Time Allowed For Cold Storage) using the properties *ep-plan:satisfies* and *ep-plan:violates* to describe whether or not these constraints were complied with during the delivery. As illustrated in **Figure 6**, the property *prov:wasInfluencedBy* links the high level delivery activity to the more detailed execution trace.

An example of more detailed plan defining the delivery process, and a corresponding execution trace is illustrated in **Figure 8**. This plan consists of three steps—*cold storage*, *ambient temperature storage*, and *receipt of delivery*. The cold storage and ambient temperature storage steps have associated HACCP constraints which refer to the maximum temperature allowed for food items stored in these stages of the delivery workflow. The food items are denoted as variables of type *fs-prov:PhysicalObject* and linked as inputs and outputs to the corresponding steps of the workflow. The result of the delivery process, which represents the action performed on the mobile app by the person receiving the delivery (i.e., pressing the accept or reject button) is also recorded.

The corresponding execution trace documenting a single execution of this plan is described using *ep-plan:Activity* and *ep-plan:Entity* concepts which are mapped as subclasses to the core PROV-O concepts *prov:Activity* and *prov:Entity*. These elements of the execution trace are wrapped in an *ep-plan:ExecutionTraceBundle* which is linked to the plan via the *prov:wasDerivedFrom* relationship (see **Figure 6**). Note that after the delivery workflow is executed (e.g., multiple deliveries fulfilled) multiple execution traces corresponding to the same plan would exist.

Since the food items are transitioning through different stages that the entities represent (e.g., food stored in cold and ambient temperature storage) these entities would not exist at the same time (i.e., food cannot be chilled and not chilled at the same time). To record the transition times data properties *prov:generatedAtTime* and *prov:invalidatedAtTime* (not shown in **Figure 8**) are used to annotate the entities with timestamps to capture the times when a food item was in the state described by the plan variable to which the entity corresponds. The entities in the execution trace are also annotated with the delivery ID using the *proofd:deliveryID* (not shown in **Figure 8**) to associate the delivery items with specific delivery orders.

4.4.2. Modeling Sensing Provenance

The IoT monitor uses temperature measurements and timestamps associated with different stages of the food delivery workflow to evaluate compliance against predefined constraints. To capture this information (i.e., how and by whom these constraints were generated) we use the *ep-plan:ConstraintEvaluation* concept based on the N-ary relations approach (Rector and Noy, 2006) to qualify the *ep-plan:satisfies/violates* relationships between execution activities and plan constraints (see **Figure 9**). This concept is then linked to the agent (in our case the IoT monitor) that performed

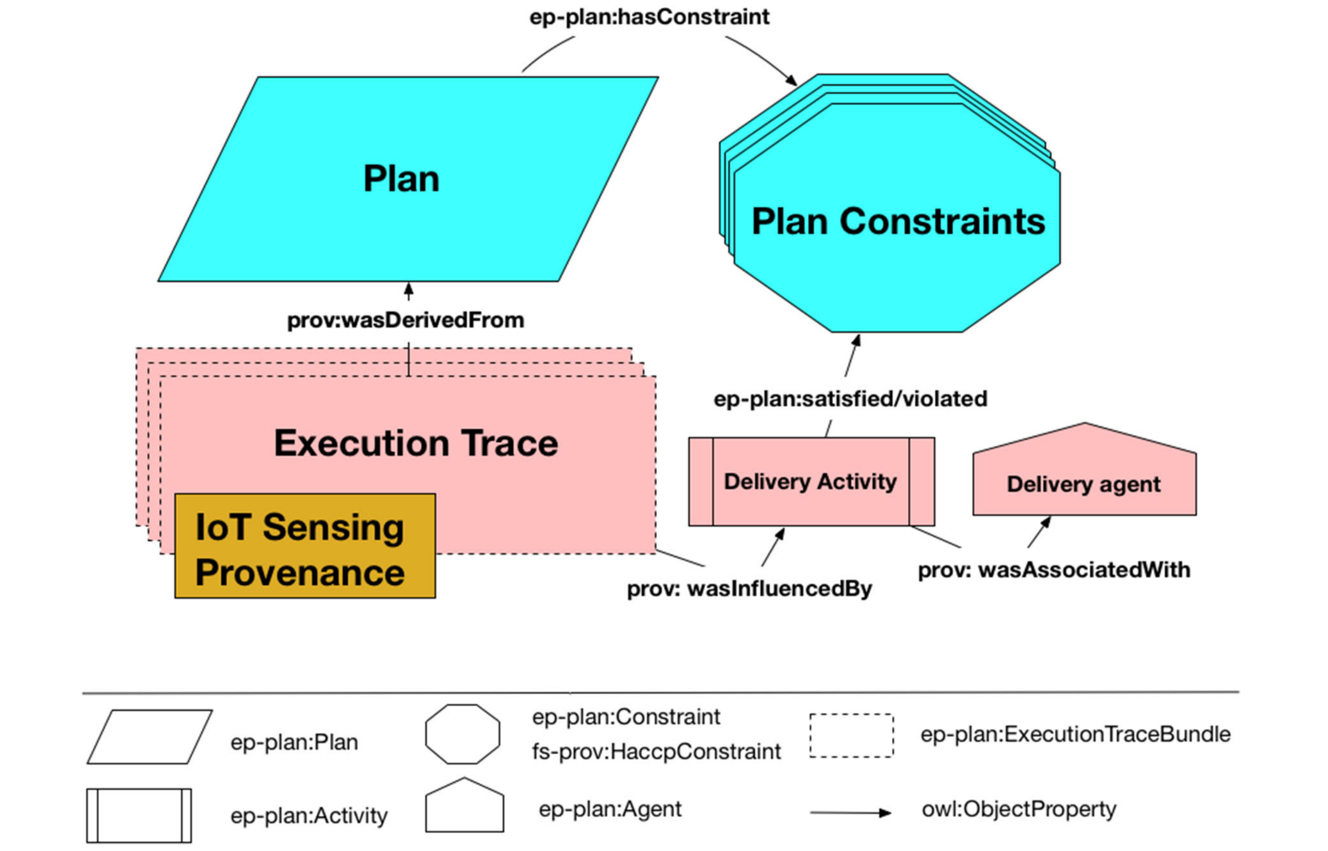


FIGURE 6 | A high level overview of the main components of the provenance record describing food delivery processes in the PROoFD-IT system.

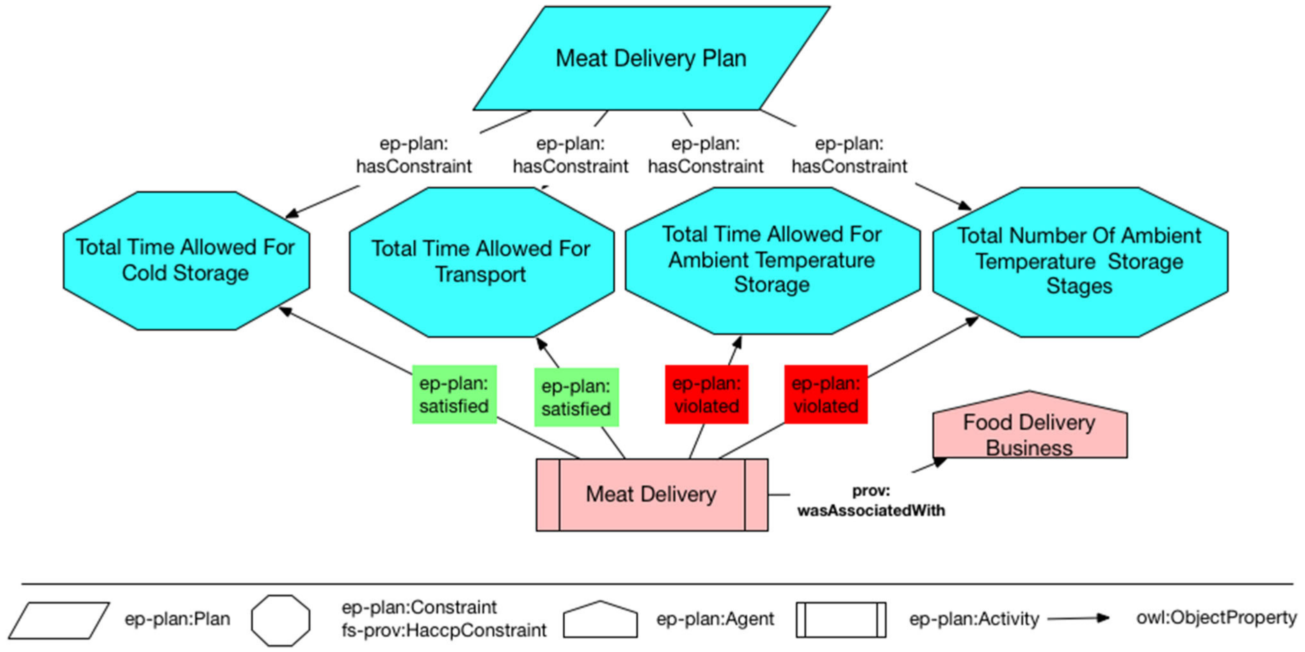


FIGURE 7 | An overview of the high level constraints associated with the delivery plan and their relationship to the high level food delivery activity.

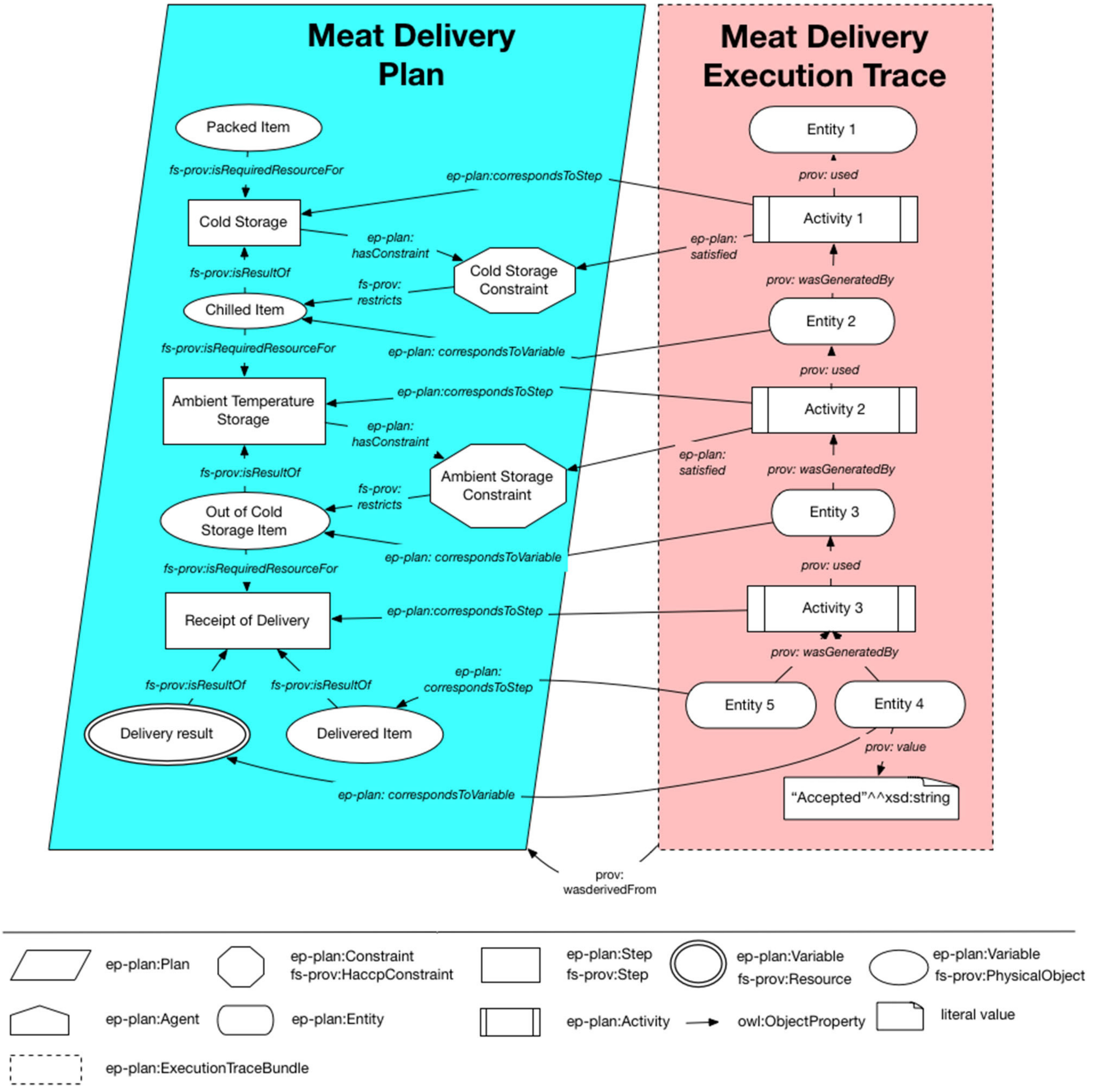


FIGURE 8 | A detailed description of a delivery plan consisting of three steps (*cold storage*, *ambient temperature storage*, and *receipt of delivery*), variables denoting the food items, associated HACCP constraints and matching execution trace.

the assessment using the *proofd:assessedBy* property. To also record information about the readings used to evaluate constraint compliance, *ep-plan:ConstraintEvaluation* is linked to an instance of *proofd:ObservationCollection* using the *proofd:basedOn* property. The concept *proofd:ObservationCollection* represents an aggregated view of all the temperature readings related to the activity corresponding to an *fs-prov:HaccpStep* and to which the evaluated constraint applies (e.g., all the temperature readings collected during cold storage that were used to evaluate a cold storage constraint). This collection is recorded as the result of an *fs-prov:MultiSensingActivity* which is also a subclass of *prov:Activity* and *sosa:Observation*. The aggregated view of observations was introduced because the IoT monitor does not store temperature observations that are below the constraint threshold. Therefore, it would not be possible to use the standard approach offered by the SOSA ontology where each observation is modeled individually. If an observation is stored (i.e., in case a constraint violation was detected) it is linked to the collection

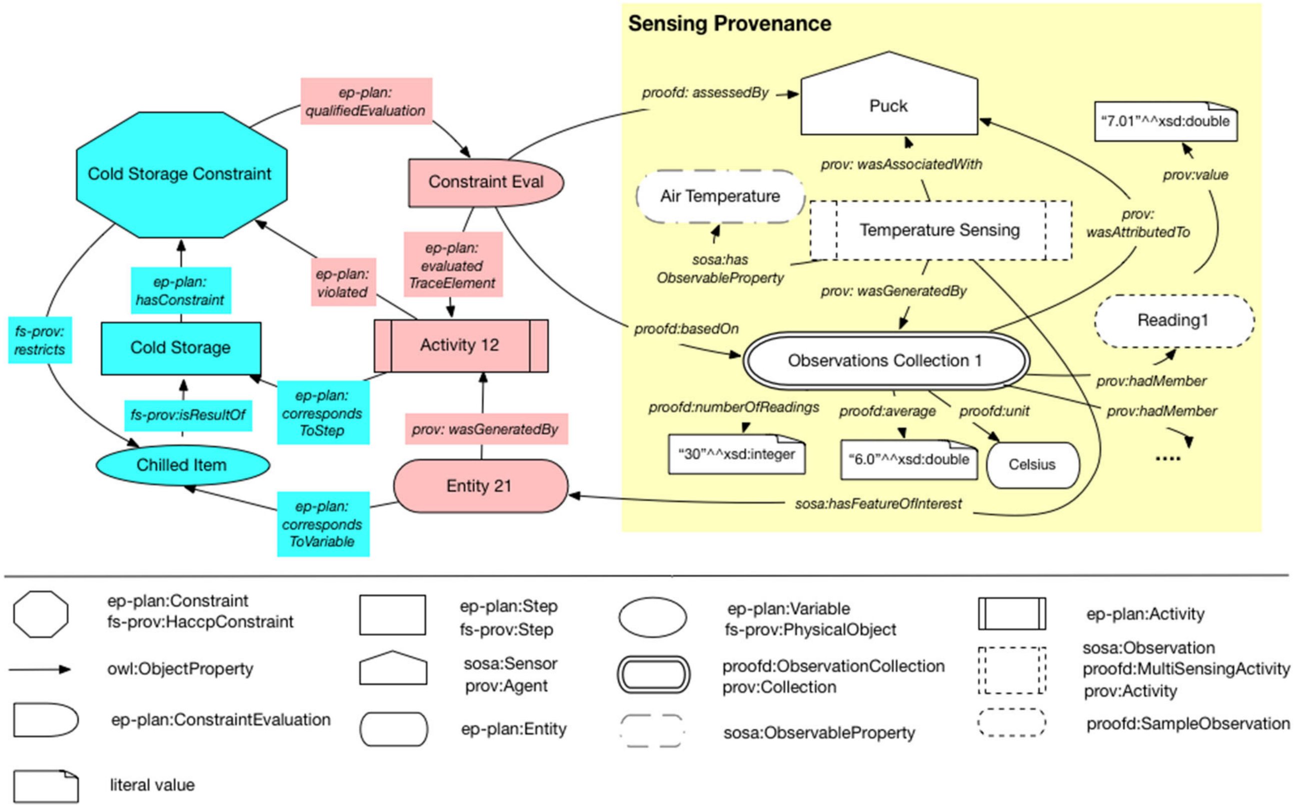


FIGURE 9 | An example record illustrating the use of the *ep-plan:ConstraintEvaluation* concept to link elements describing additional sensor information (e.g., number of sensor readings, units of observation, etc.) and documenting the context in which a constraint was evaluated.

using the *prov:hadMember* property. The observation collection is further annotated with aggregated statistics, such as the computed average of all readings, number of readings made, and the unit corresponding to the readings (i.e., the degrees Celsius unit defined in the Units of Measure ontology[20]). The concept *sosa:ObservableProperty* is used to describe the property (e.g., air temperature) that was observed by the sensor. This relates to the entity (*Feature of Interest*) that is the subject of the observation activity (e.g., air temperature around the chilled item entity).

By using the vocabulary introduced in the W3C SSN ontology we are able to link elements in the provenance record, for example the sensor making the observations, to richer static descriptions of device capabilities, such as range, accuracy, the specific type of sensor used, etc.

4.5. Blockchain Network and API

Provenance data produced by the server app are stored in an immutable, distributed ledger, ensuring transparency and authenticity of information. Hyperledger Composer framework was used to manage a blockchain network node based on Hyperledger Fabric. The Hyperledger Fabric can be described as a private blockchain network, with most of its real-world applications in B2B scenarios. It does not feature any rewards for adding extra blocks to the chain, thus provides no incentive for miners to perform any work, rather it leaves this burden on businesses setting up and configuring the node. This type of network is beneficial for scenarios where the data needs to remain private and should not be exposed to public audiences. The operations on the network are defined through a smart contract constructed using three main concepts: *participants*, *assets*, and *transactions*. Participants represent the agents, such as food manufacturers or delivery services participating in the network. Assets represent the actual items that are subjects of transactions, e.g., a box of sandwiches. Transactions define events which affect assets, for example delivery of Y from A to B, where Y is the asset and A,B are the participants, causing changed ownership of Y. The following simple smart contract was defined using the Hyperledger Composer modeling language[21] to support testing of blockchain integration within the PROoFD-IT system:

- **BusinessEntity** (participant)
  - ⋆ *String* businessId
  - ⋆ *String* businessName
- **Commodity** (asset)
  - ⋆ *String* tradingSymbol

[20] http://www.ontology-of-units-of-measure.org/resource/om-2/degreeCelsius

[21] https://hyperledger.github.io/composer/v0.19/reference/cto_language.html

- ⋆ *String* description
- ⋆ *BusinessEntity* owner (current owner of the item)
- ⋆ *String* status (whether the item has been accepted or rejected)
- ⋆ *String* complianceReport

- **Delivery** (transaction)
  - ⋆ *Commodity* commodity (item to be transferred)
  - ⋆ *BusinessEntity* newOwner (BusinessEntity to which the ownership is going to be transferred)
  - ⋆ *String* status (whether the delivery has been accepted or rejected)
  - ⋆ *String* complianceReport.

In summary, the smart contract defines one transaction (*Delivery*) which records the change in ownership of a delivered item (*Commodity*) defined by id and a short textual description. The current owner and current status of the commodity is updated as part of the delivery transaction generated by the PROoFD-IT system at the end of the food delivery process. In addition, the commodity is associated with a semantic provenance graph (exported as text and stored in the *complianceReport* attribute) describing the food safety compliance report generated by the PROoFD-IT system as described in the previous section.

5. EVALUATION OF THE CORE HARDWARE COMPONENTS OF THE PROoFD-IT SYSTEM

In this section, we report the results of our in-house evaluation of various hardware components of the PROoFD-IT system. This evaluation was performed as a series of experiments at different stages of the PROoFD-IT system development cycle. A domestic fridge was used to simulate conditions in a cold store. Results highlight a number of issues which should be of relevance to developers and policy makers considering similar systems which utilize battery powered and resource constrained IoT devices in the food safety context.

5.1. Temperature Sensor Accuracy

To better understand the accuracy of our IoT monitor in terms of temperature observations, we compared it against the Tinytag TGU-4017 temperature data logger[22] (purchased with a calibration certificate). We tested two versions of the IoT monitor, one with the built-in internal temperature sensor (with reported accuracy ±1°C [23]) and one with the DS18B20 temperature probe attached. All three sensors were initially kept at ambient temperature, then placed in a domestic fridge for a period of 3 h, and then returned back to ambient temperature. **Figure 10** shows that neither of the IoT monitors reported the same temperature observations as the certified logger. Results did however suggest that the IoT monitor reacts faster in detecting temperature changes. The IoT monitor using an internal sensor produced more irregular readings than the external probe and the certified logger; in addition, it produced varying offsets at different temperatures (when compared against the certified logger), possibly due to low sensor accuracy (±1°C). However, the version with the DS18B20 probe did exhibit a more stable pattern of temperature readings, which was closer to the one reported by the certified logger and was therefore selected for use in the trials discussed below. When benchmarked against the certified temperature logger, **Figure 10** suggests that both versions of IoT monitors would not meet the requirement of deviations of no more than ±0.3°C when the instrument is operated at temperatures of −20 to +30°C as defined in the Food Law Practice Guidelines (England) (Food Standards Agency, 2017) (see more details in section 2). The IoT monitor internal sensor would also fail the requirement for reported accuracy ±0.5°C due to its reported accuracy of ±1°C.

The temperature detected by a sensor can clearly be influenced by other factors, such as position. For example, if located inside a box, it will take longer for the detected temperature to drop to the levels of the outside air temperature maintained by the cooling appliance which the PROoFD-IT system is designed to observe. This is due to the sensor observing the air temperature inside the box which will depend on the mass and the thermodynamic properties of the food item and the storage box walls as these will influence the heat transfer between the warmer box and the outside air of the cooling appliance (Raval et al., 2013).

During initial tests, we used a plastic box filled with bread and placed it in a domestic fridge for 3 h. **Figure 11** compares different temperature observations recorded by the certified temperature sensor and two IoT monitors. We observed that it could take as long as 2 h for an IoT sensor to start reporting a temperature below 5°C if placed inside a closed box; as expected, a temperature sensor placed on the outside of the box reported the correct air temperature significantly faster. The correct air temperature was also reported within the pre-configured alert period set on the IoT monitor to avoid triggering false non-compliance alarms when the food items are cooling down (see section 4.2).

5.2. Battery

Manufacturers often advertise that battery powered IoT devices can operate for months without the battery needing to be replaced. For example, the Puck.js is advertised with "a year-long battery life on a common CR2032 battery[24]." However, this is highly dependent on the software running on the device and the resources used. During initial testing we found that the use of LEDs and Bluetooth has to be carefully managed, and even without any use of LEDs and careful timing of Bluetooth scans (to look for location beacons to detect the current position of the IoT monitor), the battery performance was reduced to days rather than months.

In addition, the battery voltage and capacity are negatively influenced by the lower temperature levels due to a decrease in the ionic conductivity and a slowdown of electrochemical reactions in certain battery components (Zhang et al., 2003).

[22] http://gemini2.assets.d3r.com/pdfs/original/3767-tgu-4017.pdf

[23] https://www.espruino.com/Puck.js

[24] https://www.puck-js.com/

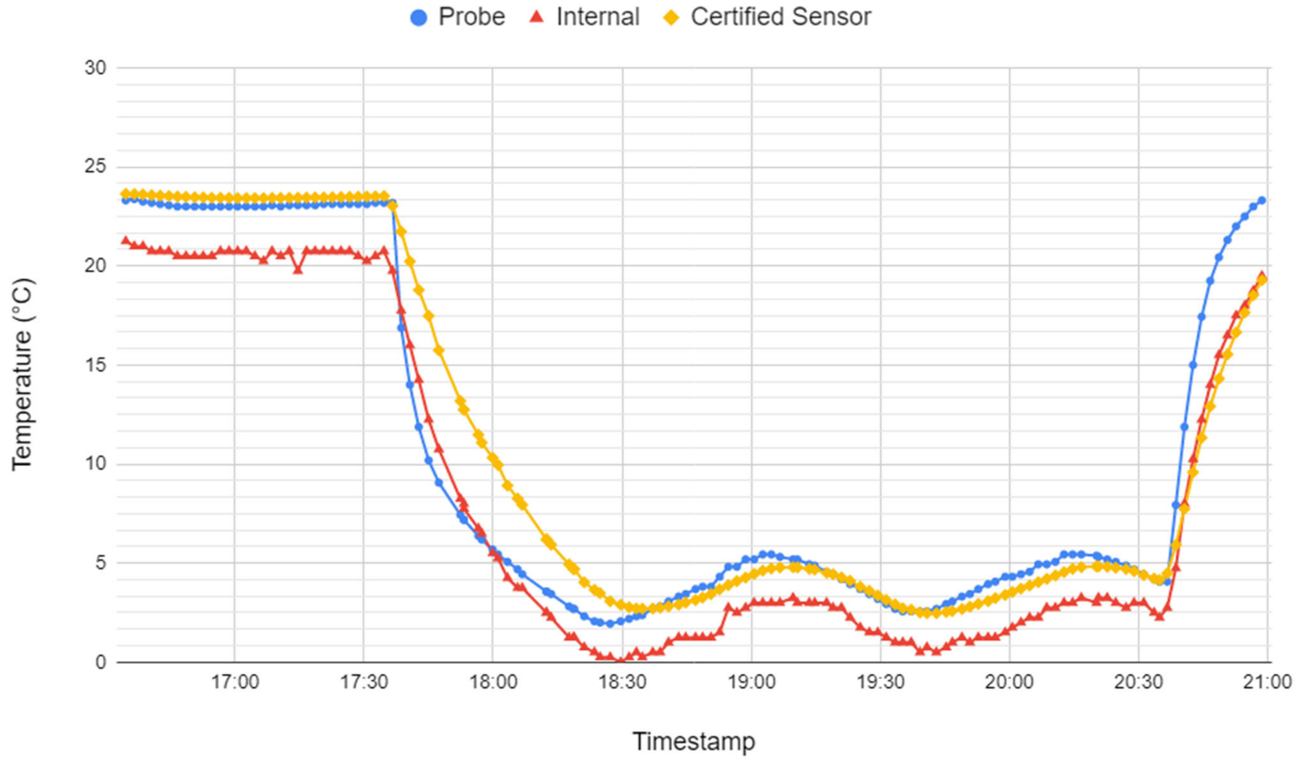


FIGURE 10 | A comparison of temperature sensor readings for two versions of the IoT monitor (one using an on-board sensor and the other with the DS18B20 probe attached) against certified temperature logger measurements.

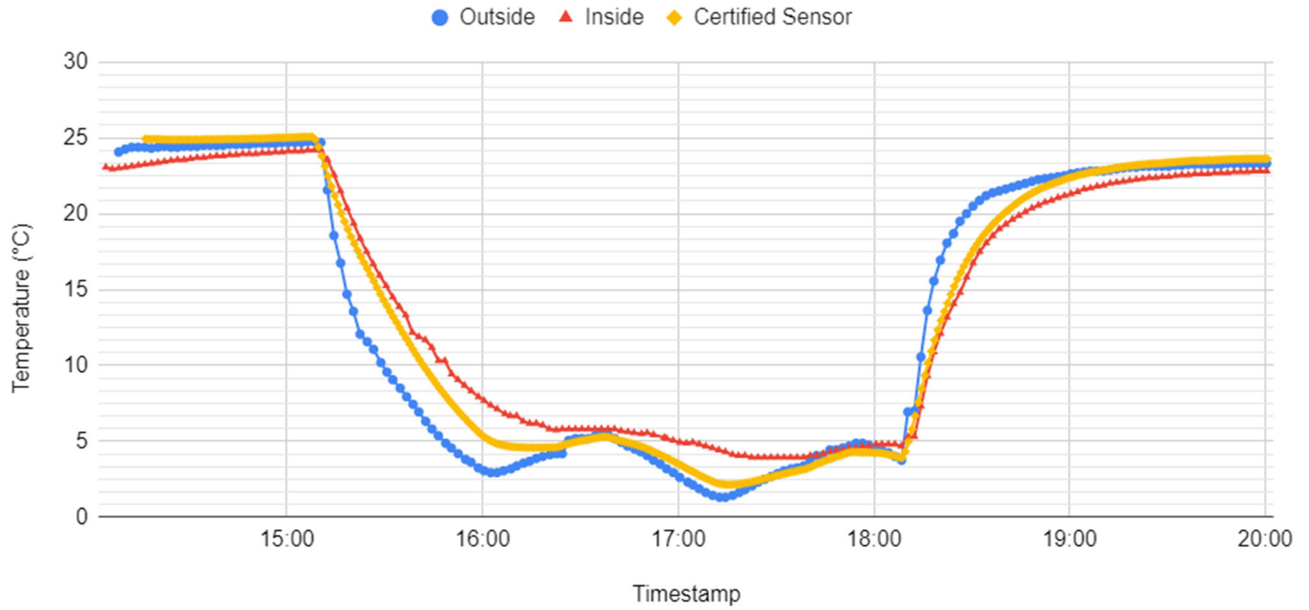


FIGURE 11 | A comparison of temperature between readings from IoT monitors with the sensing probe placed on the inside and on the outside of a delivery box and from certified temperature sensor placed on the outside.

Figure 12 illustrates the battery levels (triangles) reported by the IoT monitor (right y-axis) under different temperatures (circles) measured by the certified temperature logger (left y-axis). Various drops in reported battery levels are clearly correlated to the decreasing temperature after the sensor has been placed in a cold storage unit. After the sensor was returned to ambient temperature, the battery levels were again reported at 100%.

5.3. Connectivity

In our system, the Bluetooth connection between the mobile app and the IoT monitor has proven to be slow and unreliable with larger JSON payloads (e.g., containing many temperature readings for non-compliant stages lasting long periods of time). As this would hinder the user experience when retrieving the data using the mobile app, we set a maximum limit on the number of readings that can be stored for each non-compliant stage, in order to manage the size of the transferred JSON payload.

Another issue we encountered was related to the Bluetooth beacons used to determine the location of IoT monitors. We found that it was difficult to estimate how the Bluetooth signal would propagate through different environments. For example, if the strength of the signal of the beacon was set too low, it was possible that an IoT monitor would not detect the beacon if the cold storage room was too large and the devices were far apart. On the other hand, if the signal was stronger, an IoT monitor positioned outside cold storage (e.g., in a corridor) would occasionally detect the beacon (e.g., when the doors of a walk in fridge were open). This would be problematic for a real system deployment as it would be difficult to estimate correct settings for all possible building and storage room layouts used by the organizations in such a heterogeneous environment as the food industry. This could potentially render the use of Bluetooth in this context impractical.

6. PROoFD-IT PROTOTYPE EVALUATION IN B2B DELIVERY SETTING

6.1. The G. McWilliam Use Case

The development process of the system included an initial prototype phase during which the base capabilities of the intelligent IoT monitor and mobile app were evaluated in a real delivery setting. This was conducted in conjunction with our partners G. McWilliam, who undertake deliveries in a business-to-business context. The trial scenario included a delivery of raw meat products that represent a typical order as delivered by the company. These deliveries were carried out alongside real deliveries to University Catering Services at the University of Aberdeen (a customer of G. McWilliam). The plan for this delivery consisted of four steps, namely cold storage (meat orders are stored in a chilled area after being prepared), removal from the storage step (outside stage), delivery step (transport in a refrigerated delivery van temperature controlled to below 5°C), and the customer receipt step. The delivery plan assumes that once food is in the chilled storage area, it should only be removed for the purposes of delivery (i.e., there should only be one outside stage).

6.2. Methodology

In this evaluation we were interested in answering two main questions:

- Can the system accurately detect compliance during a real delivery process?
- Do suppliers and business customers find the concept and proposed operation of the PROoFD-IT system useful?

These questions were addressed through two trials carried out with both our named partners as the University of Aberdeen Catering Service acted as a recipient of the food deliveries in this evaluation process. These trials included interviews with individuals who observed the initial trials; one as the supplier overseeing the delivery process, and one as the business customer accepting the delivery. The first question was evaluated through manual comparison of events detected by the IoT monitor and the detailed temperature log produced by the certified temperature logger, as well as the overall functionality of the system. The second question was evaluated through qualitative feedback from participants observing the test scenario.

To test the ability of our system to detect compliant and non-compliant events during the delivery stage we tested the following:

- [compliant] The delivery process was uninterrupted and the meat stored and delivered as per the usual delivery process.
- [non-compliant] The meat was removed from the chilled storage area for a period of 3 h during the storage period, and replaced prior to delivery.

The PROoFD-IT system (together with a certified temperature logger) was deployed to test the compliant scenario in November 2019 and the non-compliant scenario in December 2019. On each occasion, a package of meat was prepared by McWilliam, stored overnight and in the morning the delivery fulfilled to the University of Aberdeen Catering Service, where it was received by a member of the project in conjunction with a representative of the Catering Service.

6.3. Results

6.3.1. Accuracy of Temperature Measurements and Reliability of Data Processing

In the first deployment, the readings from the IoT monitor correctly identified the delivery item moving through two stages of the delivery workflow (i.e., cold storage and transport). Interestingly, the outside stage when food was removed from the cold store and subsequently placed in the delivery van was not detected by the IoT monitor. This was due to the speed with which this transfer occurred, meaning that it fell between the IoT monitor's periodic scans for location beacons. The delivery was correctly assessed as compliant because no temperature constraints were breached which was confirmed by the temperature readings collected by the certified temperature logger.

In the second deployment, we observed that the IoT monitor was unable to reliably detect the duration of the outside stage when the food item was removed from the cold store. This was due to the device being placed relatively close to the cold store.

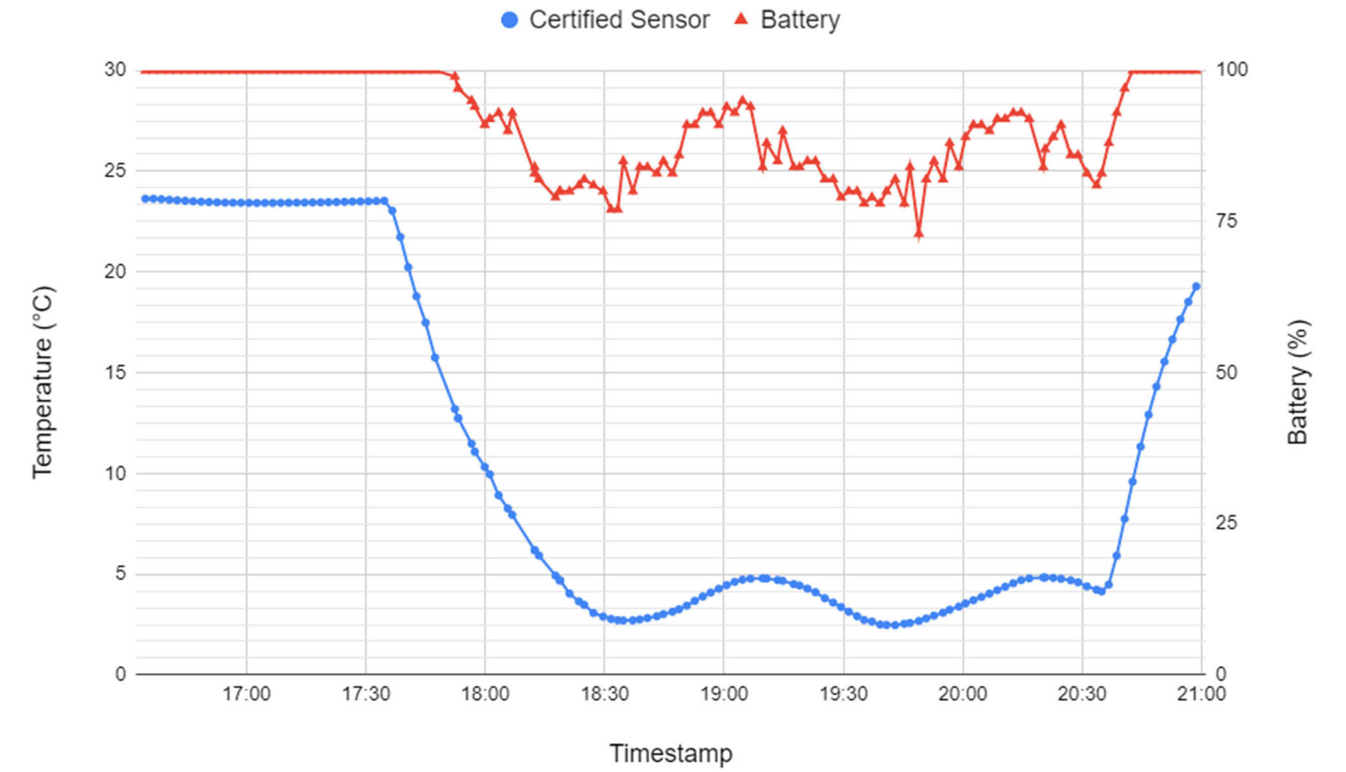


FIGURE 12 | A comparison between temperature recorded using the certified temperature sensor (circles) and battery percentage (triangles) reported by the IoT monitor.

As a result, the IoT monitor often detected the location beacon inside the cold store which lead to it recording an inaccurate list of multiple delivery stages (i.e., *fridge* and *outside*) indicating that the food item was frequently removed and placed back into the cold store. We also observed that even during the period when the food was kept in the corridor outside of the cold storage (i.e., away from the location beacon) the temperature was still recorded below the 5°C threshold for cold storage, due to low overnight environmental temperatures. Therefore, despite the food item being out of the cold store it was still technically stored in compliance with HACCP temperature constraints (as if it was in a cold store). However, our IoT monitor would assess this situation as non-compliant due to the food item being treated as if it were in the *outside* stage, and it exceeding the constraint defining the maximum permitted duration of that stage.

6.3.2. User Perceptions

Both interviewees, representing the supplier and customer end of the process, were positive regarding the system and its potential benefits. They both mentioned that such systems would reduce the amount of paperwork currently required to maintain temperature records, and make it easier to review and search records in a digital form. The supplier representative suggested there would be little negative impact on their normal processes if such a system were implemented, since the devices were unobtrusive and easy to use. This was echoed by the customer representative who noted that they already take temperature readings when food arrives, so the use of the app would not create additional work, and that being able to see that the device had traveled with the food throughout the process would provide reassurance. The supplier suggested that benefit would be gained through confirming that assumptions about conditions of storage and transport are correct, useful for both them and their customers. Similarly, the customer representative described positive benefits that would arise if this system were implemented across the sector and for all deliveries that were made. They discussed how, under the current system, it was impossible to know if temperature standards had been breached during the delivery process due to, for example, frequent opening of the chilled space during multiple deliveries. Both mentioned that the system addressed concerns that currently could arise due to gaps in the supply chain and temperature measurement.

7. PROoFD-IT PROTOTYPE EVALUATION IN B2C DELIVERY SETTING

7.1. The University of Aberdeen Catering Service Use Case

Evaluation of the full PROoFD-IT system (including the server app producing provenance annotations and the blockchain network) was performed in conjunction with our second project

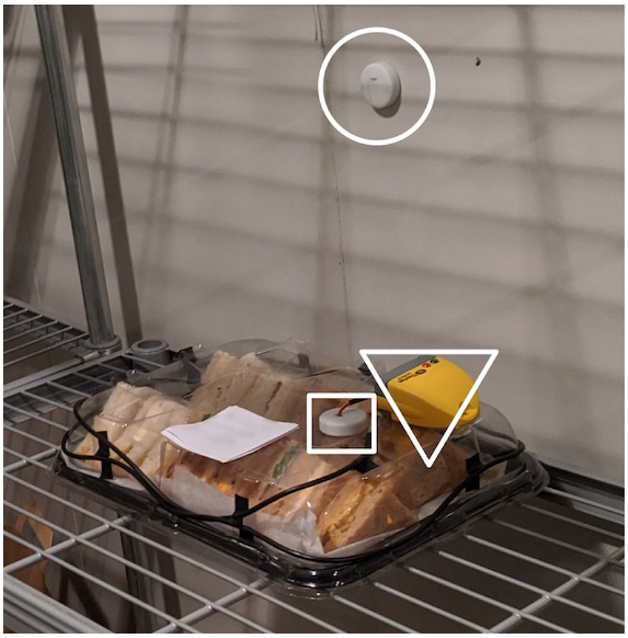


FIGURE 13 | A sandwich box used in the trials with the university catering services. The fridge beacon is highlighted with a circle, the IoT monitor with a square, and the certified temperature logger with a triangle.

partner, the University of Aberdeen Catering Service.[25] The trial scenario included a delivery of sandwich boxes (see **Figure 13**) that represent a typical food service for various on-campus events, such as meetings, workshops, etc. The plan for this delivery consisted of three steps, namely cold storage (sandwiches are stored in the fridge after being prepared), outside step (deliveries occurring at ambient temperature), and the customer receipt step. The delivery plan assumes that once food is in the fridge, it should only be removed for the purposes of delivery. The delivery has to complete within 4 h from the time when food was removed from the fridge to comply with the 4 h rule (i.e., food intended for direct consumption can be left outside a temperature controlled environment, but should be consumed within 4 h) (Food Standards Agency, 2016).

7.2. Methodology

In this evaluation we were interested in answering three main questions:

- Can the system detect accurately non-compliance during a real delivery process?
- Do users without professional food safety knowledge find the information provided by the PROoFD-IT mobile app useful?
- Is it possible to store, retrieve and query stored provenance records from the blockchain network to reproduce the information produced by the IoT monitor and the mobile app?

The first question was evaluated through manual comparison of events detected by the IoT monitor and the detailed temperature log produced by the certified temperature logger. The second question was evaluated via a survey conducted with participants who received and inspected the sandwich deliveries using the PROoFD-IT app. The survey collected both qualitative and quantitative data, and was conducted digitally following the trials. For the third question, we constructed a number of provenance queries using the SPARQL query language (see section 7.3.3) to test if important pieces of information (e.g., violation of individual constraints during delivery stages) can be retrieved from the semantic provenance graphs stored on the blockchain.

To test the ability of our system to detect compliant and non-compliant deliveries we tested the following scenarios:

1. [compliant] Sandwiches are packed into a box and placed in a fridge. After some time these are then removed from a fridge and delivered to a specific location on the campus.
2. [non-compliant] Sandwiches are packed into a box and placed in a fridge. At some point the sandwiches are removed from the fridge and left at ambient temperature for a minimum of 3 h. Then they are placed back in the fridge. After some time they are removed from the fridge and delivered to a specific location on the campus.
3. [non-compliant] Sandwiches are packed into a box and placed in a fridge. At some point the sandwiches are removed from the fridge and left at ambient temperature for a minimum of 3 h and then delivered to a specific location on the campus.

The boxes were delivered to selected participants (not affiliated with the project) who then used the PROoFD-IT mobile app to inspect the delivery. Each delivered sandwich box contained one smart IoT monitor and a certified temperature logger for reference. The PROoFD-IT system was deployed for 9 days in March 2020. Each day one sandwich delivery to a different location on the university campus was fulfilled by the University Catering Service, with details of the storage and delivery process in accordance with one of the three scenarios outlined above. Each scenario was tested three times. All deliveries were purchased directly by the project and discarded after the trial due to the nature of the scenarios (i.e., testing non-compliance).

7.2.1. Participant Recruitment

People managing the delivery process were all members of staff from the University Catering Service (a separate business unit operating within the University of Aberdeen). People receiving deliveries were recruited through a university mailing list and were paid a small cash sum for their time. A total of nine people were recruited, eight of whom were university staff and one PhD student. To be considered for the study, volunteers were asked whether they had experience with receiving food deliveries from the University Catering Service in the past (e.g., for a workshop, meeting, etc.). Every participant was briefed about the purpose of the trials and were given an opportunity to withdraw from the study at any time.

[25] https://www.abdn.ac.uk/staffnet/working-here/delivered-catering-442.php

TABLE 1 | Mean responses to questions where 1 = strongly disagree, 5 = strongly agree.

Question	Mean
The app was easy to use.	4.67
I think I would like to use this app in the future.	4.34
I found the app unnecessarily complex.	1.22
I think that I would need the support of a technical person to be able to use this app.	1.11
The app functionality and the information it provided were useful.	4.56

7.3. Results

7.3.1. Detecting Compliance and Non-compliance

The system performed well and delivered expected compliance assessments in all but the first trial. During the first test of a compliant scenario the sandwiches were placed into a small fridge located in the storage room. The IoT monitor recorded a number of readings slightly above the 5°C threshold which were also confirmed by the certified logger reporting an average of 5.5°C during the cold storage stage.[26] The fridge was operating normally and the observed readings above the 5°C threshold were within the sensor's accuracy limits. However, due to the hard constraints programmed into the IoT monitor (based on four consecutive readings above the 5°C threshold—see section 4.2), this stage was deemed non-compliant. In the interest of avoiding borderline cases the remaining trials were performed in a large walk-in fridge where the temperature was maintained at 1–4°C.

Trials testing non-compliant scenarios also included shorter cold storage periods of <1 h. For these periods both the IoT monitor and the certified logger reported average temperatures above 5°C which did not accurately reflect the air temperature inside the fridge. This is consistent with the observed behavior of both sensors which require time to cool down in order to start measuring the air temperature that the appliance is set to maintain (see discussion in section 5.1). The differing reaction times and sampling periods of the IoT monitor and the certified logger also caused the average values reported by the sensors to differ significantly. While the IoT monitor only collects observations every 7–20 min, the certified logger was set to collect one observation every minute. The IoT monitor also reacted faster to changes in temperature. The average values reported by both sensors were therefore influenced differently in situations when food was moved between warmer and colder environments for shorter periods.

7.3.2. User Survey

The user survey included a number of questions which investigated user satisfaction with the PROoFD-IT mobile app and the general idea of an IoT-based food safety monitoring system. Overall results suggested that participants reacted positively to the app (see **Table 1**). Qualitative responses supported these findings, with participants commenting on the ease of use and straightforward nature of the app, and the fact that it did not require any specialist knowledge.

Participants were asked whether the app made them feel more or less confident in their knowledge about the safety of the food, with responses from 1 (much less confident) to 5 (much more confident). The mean result was 4.67 indicating that the app had a highly positive impact on confidence. Asked if they would like to have this service available for future deliveries, all of the participants gave a positive response. Several mentioned that such a system would provide additional information about the food and delivery process that would be of use to them, for example: "*it made me realize that we don't know what happens with our food before it arrives*" and "*we really don't know how long food has been left out prior to it getting here*." Two participants described how such a system would impact their own decision making beyond whether or not to accept the delivery, but about how long after delivery the food would be safe to eat: "*A lot of our use for catering deliveries is for drop in lunches, so food would be laid out for a while. This service would be useful so we can know how long the food has been acceptable before arrival to then impact how long we should make the food available to delegates*." When asked about their confidence in the data provided by the app, all participants indicated high level of trust in the food safety data provided. For example, "*I would trust it 100 percent as it gives exact details*."

Of the nine deliveries completed, six took place under conditions where the food did not meet the minimum requirements to be compliant with food safety standards, due to being removed from the fridge either during the storage stage, or for more than 4 h during the delivery stage. A further delivery did not satisfy compliance criteria because the temperature of the fridge did not meet the necessary standards. Two study participants were informed by the app that the food was compliant, and the remaining seven were informed that it was not. Interestingly, only one participant declined to accept the delivery, for reasons we shall discuss below. Despite this, most participants indicated that the information provided by the app would highly influence their decision making on accepting deliveries, with a mean response of 4.33 (1 = low influence, 5 = high influence).

We asked the participants whether they examined the detailed data giving information about the delivery stages. All of the participants said that they had looked at this, and three of them specifically noted that based on the detailed temperature information provided, they had decided to accept the delivery even though the system flagged it as non-compliant. For example, one participant noted: "*I looked at the stages and accepted the delivery despite it not meeting the temperature guidelines as it was only one degree above the fridge temperature*." This finding was emphasized by answers to a question where we asked participants if they could imagine any circumstances where they might accept food which was described as being not acceptable. While two of the respondents said they would always reject such food, the remainder of the participants described circumstances where they would make an individual decision informed by the information provided, for example: "*It could say it was not*

[26] The average was calculated from readings obtained every 1 min during 4 h period in the cold storage. The readings obtained from the logger during the initial 45 min were ignored to eliminate the period when the sensor was cooling down.

acceptable because it had been out of the fridge but the temps in the room are colder than the fridge which would mean it would be acceptable to take the food." Several participants also mentioned that the type of food would impact their decision making, for example if it was food which was more or less susceptible to dangerous bacterial growth.

Because we were interested in overall impacts on food safety understanding, we also asked participants whether the use of this app would be likely to change their views or behavior around food safety. Six out of the nine responses suggested that positive behavior changes would take place, with responses suggesting that their awareness of the issues surrounding food safety and information available were key to these changes. One further response was ambivalent about whether changes would take place, with another noting that their level of awareness was already high so no changes would be necessary. We also asked whether the participants learned anything about food safety guidelines from participating in the trial. Seven participants responded that they did learn about food safety, with four specifically mentioning temperature related guidelines, for example "*I learned about suitable temperatures, putting food in and out of different fridges*." Some participants also mentioned that they had learned about the various stages that food goes through before being delivered.

7.3.3. Evaluation of Provenance Annotations

To evaluate whether the server application produces correct semantic provenance annotations, a sample provenance graph was tested against a set of competency questions, which is a common method for evaluating ontologies (Grüninger and Fox, 1995). These were designed to test the various parts of our provenance model and included the following questions:

- Q1: Which HACCP constraints associated with the overall plan were satisfied/ not satisfied?
- Q2: Who was responsible for the delivery?
- Q3: Which activities breached the HACCP constraints associated with planned HACCP steps?
- Q4: What was the number of sensor readings made, average values, and unit of measurement for each temperature controlled step?
- Q5: What observable property and what feature of interest was used by the sensor to produce temperature observations?
- Q6: Which steps were executed more than once in a single execution trace?
- Q7: Which sample readings were recorded for activities that breached HACCP temperature constraints associated with planned HACCP steps?
- Q8: How long was the tracked food item in the delivery process?
- Q9: When was the item received by the customer?
- Q10: Was the item accepted/rejected by the customer?

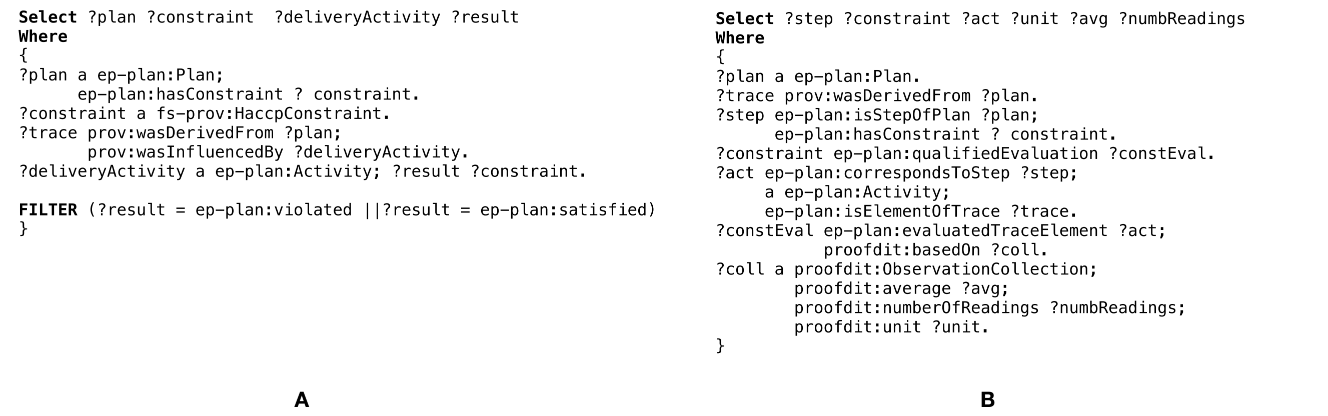
The competency questions were formalized as SPARQL queries and executed against a semantic graph produced by the server application from a JSON payload recording a non-compliant food delivery following the two stage plan (i.e., containing *fridge* and *outside* stages) used in the trials. Two sample SPARQL queries are illustrated in **Figure 14**. Query A corresponds to Q1 and returns the list of constraints associated with the overall plan, such as *total time allowed for cold storage*, *total time allowed for ambient temperature storage*, *total number of allowed ambient temperature storage stages*, and whether these constraints were satisfied by a specific delivery activity (see section 4.4.1 for related information). In the same figure, Query B corresponds to Q4, returning the details on how a specific constraint was evaluated based on sensor readings (see section 4.4.2 for related information).

We evaluated our questions against a provenance record produced by an example non-compliant scenario with a mixture of satisfied and violated HACCP constraints. Violations cause the IoT monitor to report richer provenance information—by including sample sensor readings demonstrating non-compliance. All queries returned the expected results. The code to re-run the evaluation, SPARQL queries, as well as the sample dataset and full results are included in the public GITHUB repository[27].

8. DISCUSSION

This pilot project has revealed a number of challenges that should be addressed before solutions, such as the PROoFD-IT system could be implemented in real delivery processes. The most prominent challenge is the difficulty of translating existing human-centered guidelines, such as HACCP into instructions that can be used by intelligent software systems. While such food safety management systems initially appear to have clear guidelines, for example, on critical temperature limits, they are first and foremost designed to be used by humans. Our experience with real world delivery workflows highlights the need for such guidelines to be much more detailed and more deterministic, clearly setting expected outcomes in various situations. For example, how long can a temperature stay above the required threshold for the food to remain compliant with the temperature controls? What is the maximum reasonable deviation of temperature readings above the maximum threshold? The need for more detailed machine-processable guidelines is necessitated by two main factors. Firstly, IoT devices provide the opportunity for collection of temperature measurements and location data about every food delivery at previously unfeasible levels of granularity (e.g., every couple of minutes). By contrast, human operators are currently expected to check the temperature only a few times per day. Secondly, software solutions require not only a set of clear constraints but expected outcomes when these are breached in a variety of ways. In the case of IoT solutions these also need to be sufficiently simple so they can be implemented on resource constrained devices. Development of such guidelines would be a complex challenge requiring inputs from different disciplines (e.g., computer science, microbiology, business, etc.) as well as policy makers responsible for regulating food industries (e.g., Food Standards Agency, Food Standards Scotland, local authorities, etc.).

[27] https://github.com/PROoFD-IT/server



```
Select ?plan ?constraint  ?deliveryActivity ?result
Where
{
?plan a ep-plan:Plan;
      ep-plan:hasConstraint ? constraint.
?constraint a fs-prov:HaccpConstraint.
?trace prov:wasDerivedFrom ?plan;
       prov:wasInfluencedBy ?deliveryActivity.
?deliveryActivity a ep-plan:Activity; ?result ?constraint.

FILTER (?result = ep-plan:violated ||?result = ep-plan:satisfied)
}
```

A

```
Select ?step ?constraint ?act ?unit ?avg ?numbReadings
Where
{
?plan a ep-plan:Plan.
?trace prov:wasDerivedFrom ?plan.
?step ep-plan:isStepOfPlan ?plan;
      ep-plan:hasConstraint ? constraint.
?constraint ep-plan:qualifiedEvaluation ?constEval.
?act ep-plan:correspondsToStep ?step;
     a ep-plan:Activity;
     ep-plan:isElementOfTrace ?trace.
?constEval ep-plan:evaluatedTraceElement ?act;
           proofdit:basedOn ?coll.
?coll a proofdit:ObservationCollection;
        proofdit:average ?avg;
        proofdit:numberOfReadings ?numbReadings;
        proofdit:unit ?unit.
}
```

B

FIGURE 14 | An example formalisation of competency questions as SPARQL queries. Query A returns the constraints associated with the overall delivery plan and whether these were satisfied by the delivery activity. Query B returns the details on how a specific constraint was evaluated based on sensor readings.

Our trials also demonstrated that inexpensive IoT technologies may under-perform not only in terms of accuracy of temperature readings, but also reliability of other functions, such as location awareness based on Bluetooth technology and battery related issues associated with operation in colder temperatures. Such weaknesses may have a particularly high impact on trust and usefulness of IoT technologies in the context of food safety solutions. As our results showed, users tend to trust information that is provided by IoT devices and are unlikely to question the accuracy or reliability of the resulting temperature observations. Should safety compliance of food deliveries be assessed on unreliable sensor readings, this could endanger public health, increase food wastage and possibly result in reputational damage to businesses.

It was demonstrated that readings from sensors that recently entered cold storage may take a significant amount of time (up to 45 min in one scenario) to identify the true air temperature inside the appliance. This can have an impact, for example, on average temperature values shown to end users for short cold storage phases (e.g., if the device manages only to produce 2–3 readings with the majority belonging to the cooling phase). As discussed in sections 5.1 and 7.3.1, such average temperature values can also differ based on the reaction times of sensors and sampling rates used. This may suggest that reporting average temperature values in this context offers little benefit to the end users and potentially increases chances of data misinterpretation. We have also observed users who ignored the system's recommendation, either based on the assumption that the reported average temperature values were only slightly higher than the recommended thresholds, or based on the "aesthetics" of the food. We suggest that further research is needed into how to efficiently communicate temperature related food safety information to non-expert users.

In terms of other practicalities, it is also clear that in a heterogeneous environment, such as the food industry, many businesses would operate different delivery plans and these would need to be translated into machine-readable form. This would lead to food business having to design machine-readable versions of their HACCP manuals (e.g., by using standard ontologies) to realize the potential of semantic technologies to support data interoperability and data standardization in the food safety context. We also propose that further investigations are required to determine whether a simple acyclic representation of plans (as presented in this article) is sufficient for most of the delivery workflows that are being deployed currently.

We also acknowledge a number of limitations of the current prototype of the PROoFD-IT system. These include the lack of authorization and security mechanisms (e.g., anyone can access the data on the IoT monitor using an app or over Bluetooth with a custom code), lack of interfaces for dynamically setting delivery ID's for individual IoT monitors, and lack of interfaces for managing and accessing information stored on the blockchain network. These limitations would need to be addressed before such a system could be released as a production ready solution.

However, despite the aforementioned challenges the overall positive response to the system from both commercial and non-commercial users may suggest that there is a demand for similar systems. The perceived benefits include increased transparency of delivery processes that lead to more informed consumer choices and enhanced monitoring by food businesses, as well as improved efficiency through reduction in paper based records and improved capability to track accountable agents in case of food safety incidents.

9. FUTURE WORK

In future work, we will explore how the PROoFD-IT system could be extended to monitor other stages in the food supply chain, such as the food manufacturing process—with an ultimate goal of achieving complete "farm to fork" solutions. This would also create an opportunity to expand our current, fairly simple blockchain model and also to test the feasibility of semantic provenance graphs to be embedded within a larger pre-existing blockchain system (e.g., as part of the aforementioned IBM Food Trust platform).

We will also explore how the availability of machine readable data can enhance automation in the food industry by utilizing machine-to-machine communication to allow oversight of the supply chain processes with more limited human interventions also focusing on management of food quality in addition to food safety.

Finally, we also aim to explore the opportunity to communicate and relay information from IoT monitors using fixed IoT beacons (e.g., in a fridge or a delivery van) to provide real-time updates. Here, the fixed IoT beacons could be connected to the Internet due to their fixed locations and potential access to mains power.

DATA AVAILABILITY STATEMENT

All publicly available software and data associated with this study can be found in the project's GITHUB repository at https://github.com/proofd-it.

ETHICS STATEMENT

The studies involving human participants were reviewed and approved by The Physical Sciences and Engineering Ethics Board, University of Aberdeen. The patients/participants provided their written informed consent to participate in this study.

AUTHOR CONTRIBUTIONS

MM, NJ, PE, and NS: conceptualization and funding application. MM and NJ: research design and survey instrument. MM and KD: software design, development, and quantitative data analysis. MM, NJ, and KD: data collection. NJ: qualitative data analysis. MM, NJ, KD, PE, and NS: writing and editing manuscript. All authors contributed to the article and approved the submitted version.

FUNDING

The work presented here was supported by an award made by the UKRI, EPSRC funded Internet of Food Things Network+ grant EP/R045127/1.

ACKNOWLEDGMENTS

We would like to thank G. McWilliam and Aberdeen University Services for their cooperation during the pilot deployments of the PROoFD-IT system. We would also like to thank Food Standards Scotland and the Semantic Web Company GmbH for their valuable comments on the project.

REFERENCES

Batlajery, B. V., Weal, M., Chapman, A., and Moreau, L. (2018). "prFood: ontology principles for provenance and risk in the food domain," in *2018 IEEE 12th International Conference on Semantic Computing (ICSC)* (Laguna Hills, CA: IEEE), 17–24. doi: 10.1109/ICSC.2018.00012

Bizer, C., Heath, T., and Berners-Lee, T. (2011). "Linked data: the story so far," in *Semantic Services, interoperability and Web Applications: Emerging Concepts* (IGI Global), 205–227. doi: 10.4018/978-1-60960-593-3.ch008

Blomqvist, E. (2014). The use of semantic web technologies for decision support–a survey. *Semantic Web* 5, 177–201. doi: 10.3233/SW-2012-0084

Bouzembrak, Y., Klüche, M., Gavai, A., and Marvin, H. J. (2019). Internet of things in food safety: literature review and a bibliometric analysis. *Trends Food Sci. Technol.* 94, 54–64. doi: 10.1016/j.tifs.2019.11.002

Caro, M. P., Ali, M. S., Vecchio, M., and Giaffreda, R. (2018). "Blockchain-based traceability in agri-food supply chain management: a practical implementation," in *2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany)* (Tuscany: IEEE), 1–4. doi: 10.1109/IOT-TUSCANY.2018.8373021

Charalabidis, Y., Alexopoulos, C., and Loukis, E. (2016). A taxonomy of open government data research areas and topics. *J. Organ. Comput. Electron. Comm.* 26, 41–63. doi: 10.1080/10919392.2015.1124720

Chen, Y.-Y., Wang, Y.-J., and Jan, J.-K. (2014). A novel deployment of smart cold chain system using 2G-RFID-Sys. *J. Food Eng.* 141, 113–121. doi: 10.1016/j.jfoodeng.2014.05.014

Department for Environment (2013). *Processed Beef Products and Horse Meat*. Available online at: gov.uk

Eckert, K., and Garijo, D. (2013). *Dublin Core to PROV Mapping*. W3C Note, W3C. Available online at: http://www.w3.org/TR/2013/NOTE-prov-dc-20130430/

Farooq, M. U., Waseem, M., Mazhar, S., Khairi, A., and Kamal, T. (2015). A review on internet of things (IoT). *Int. J. Comput. Appl.* 113, 1–7. doi: 10.5120/19787-1571

Food Standards Agency (2016). *Guidance on Temperature Control Legislation in the United Kingdom*. Food Standards Agency.

Food Standards Agency (2017). *Food Law Practice Guidance (November 2017)*. Food Standards Agency.

Grüninger, M., and Fox, M. S. (1995). "Methodology for the design and evaluation of ontologies," in *IJCAI95 Workshop on Basic Ontological Issues in Knowledge Sharing* (Montreal, QC).

Haller, A., Janowicz, K., Cox, S., Phuoc, D. L., Taylor, K., Lefrançois, M., Atkinson, R., García-Castro, R., Lieberman, J., and Stadler, C. (2017). *Semantic Sensor Network Ontology*. W3C Recommendation, W3C. Available online at: https://www.w3.org/TR/2017/REC-vocab-ssn-20171019/

Harris, S., and Seaborne, A. (2013). *SPARQL 1.1 Query Language*. W3C Recommendation, W3C. Available online at: http://www.w3.org/TR/2013/REC-sparql11-query-20130321/

Kamilaris, A., Fonts, A., and Prenafeta-BoldÚ, F. X. (2019). The rise of blockchain technology in agriculture and food supply chains. *Trends Food Sci. Technol.* 91, 640–652. doi: 10.1016/j.tifs.2019.07.034

Klischewski, R. (2015). "Semantic e-government: implementing the next generation of information and process integration," in *E-Government: Information, Technology, and Transformation: Information, Technology*, ed H. J. Schnoll (Routledge), 219–236.

Kodan, R., Parmar, P., and Pathania, S. (2019). Internet of things for food sector: status quo and projected potential. *Food Rev. Int.* 36, 584–600. doi: 10.1080/87559129.2019.1657442

Lebo, T., Sahoo, S., McGuinness, D., Belhajjame, K., Cheney, J., Corsar, D., Garijo, D., Soiland-Reyes, S., Zednik, S., and Zhao, J. (2013). *PROV-o: The PROV Ontology*. W3C Recommendation, W3C. Available online at: http://www.w3.org/TR/2013/REC-prov-o-20130430/

Markovic, M., Edwards, P., Kollingbaum, M., and Rowe, A. (2016). "Modelling provenance of sensor data for food safety compliance checking," in *International Provenance and Annotation Workshop (IPAW 2016)* (McLean, VA: Springer), 134–145. doi: 10.1007/978-3-319-40593-3_11

Markovic, M., Garijo, D., Edwards, P., and Vasconcelos, W. (2019). "Semantic modelling of plans and execution traces for enhancing transparency of IoT systems," in *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)* (Granada: IEEE), 110–115. doi: 10.1109/IOTSMS48152.2019.8939260

Moreau, L., Clifford, B., Freire, J., Futrelle, J., Gil, Y., Groth, P., Kwasnikowska, N., Miles, S., Missier, P., Myers, J., et al. (2011). The open provenance model core specification (v1. 1). *Fut. Gen. Comput. Syst.* 27, 743–756. doi: 10.1016/j.future.2010.07.005

Moreau, L., and Groth, P. (2013). *PROV-Overview*. W3C Note, W3C. Avaialable online at: http://www.w3.org/TR/2013/NOTE-prov-overview-20130430/

Moreau, L., Groth, P., Cheney, J., Lebo, T., and Miles, S. (2015). The rationale of prov. *Web Semantics* 35, 235–257. doi: 10.1016/j.websem.2015.04.001

Mortimore, S., and Wallace, C. (2013). *HACCP: A Practical Approach*. Springer Science & Business Media.

Nærland, K., Müller-Bloch, C., Beck, R., and Palmund, S. (2017). "Blockchain to rule the waves-nascent design principles for reducing risk and uncertainty in decentralized environments," in *International Conference on Information Systems (ICIS)* (Seoul).

Nakamoto, S. (2019). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Technical report, Manubot.

New, S. (2010). The transparent supply chain. *Harvard Bus. Rev.* 88, 1–5. Available online at: https://hbr.org/2010/10/the-transparent-supply-chain

OWL Working Group (2012). *OWL 2 Web Ontology Language Document Overview, 2nd Edn.* W3C recommendation, W3C.

Pal, A., and Kant, K. (2019). Using blockchain for provenance and traceability in internet of things-integrated food logistics. *Computer* 52, 94–98. doi: 10.1109/MC.2019.2942111

Patel-Schneider, P., and Hayes, P. (2014). *RDF 1.1 Semantics*. W3C Recommendation, W3C. Available online at: http://www.w3.org/TR/2014/REC-rdf11-mt-20140225/

Pearson, S., May, D., Leontidis, G., Swainson, M., Brewer, S., Bidaut, L., Frey, J. G., Parr, G., Maull, R., and Zisman, A. (2019). Are distributed ledger technologies the panacea for food traceability? *Glob. Food Sec.* 20, 145–149. doi: 10.1016/j.gfs.2019.02.002

Ram, S., and Liu, J. (2009). "A new perspective on semantics of data provenance," in *Proceedings of the First International Workshop on the Role of Semantic Web in Provenance Management (SWPM 2009), Collocated With the 8th International Semantic Web Conference (ISWC-2009)* (CEUR-WS) (Washington, DC).

Ramírez-Faz, J., Fernández-Ahumada, L. M., Fernández-Ahumada, E., and López-Luque, R. (2020). Monitoring of temperature in retail refrigerated cabinets applying iot over open-source hardware and software. *Sensors* 20:846. doi: 10.3390/s20030846

Raval, A. H., Solanki, S. C., and Yadav, R. (2013). A simplified heat transfer model for predicting temperature change inside food package kept in cold room. *J. Food Sci. Technol.* 50, 257–265. doi: 10.1007/s13197-011-0342-z

Rector, A., and Noy, N. (2006). *Defining N-ary Relations on the Semantic Web*. W3C Note, W3C. Available online at: http://www.w3.org/TR/2006/NOTE-swbp-n-aryRelations-20060412/

Reyna, A., Martín, C., Chen, J., Soler, E., and Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Fut. Gen. Comput. Syst.* 88, 173–190. doi: 10.1016/j.future.2018.05.046

Schneider, J., and Stickdorn, M. (2011). *This Is Service Design Thinking: Basics, Tools, Cases*. Wiley.

Shi, B., Sreeram, V., Zhao, D., Duan, S., and Jiang, J. (2018). A wireless sensor network-based monitoring system for freshwater fishpond aquaculture. *Biosyst. Eng.* 172, 57–66. doi: 10.1016/j.biosystemseng.2018.05.016

Shih, C.-W., and Wang, C.-H. (2016). Integrating wireless sensor networks with statistical quality control to develop a cold chain system in food industries. *Comput. Standards Interfaces* 45, 62–78. doi: 10.1016/j.csi.2015.12.004

Sylvester, G. (2019). *E-agriculture in Action: Blockchain for Agriculture (Opportunities and Challenges)*. Bangkok: FAO. Available online at: http://www.fao.org/documents/card/en/c/CA2906EN/

Tian, F. (2017). "A supply chain traceability system for food safety based on haccp, blockchain & internet of things," in *Proceedings of 2017 International Conference on Service Systems and Service Management* (Dalian: IEEE), 1–6.

Tsang, Y., Choy, K., Wu, C., Ho, G., Lam, H., and Tang, V. (2018). An intelligent model for assuring food quality in managing a multi-temperature food distribution centre. *Food Control* 90, 81–97. doi: 10.1016/j.foodcont.2018.02.030

Zhang, S., Xu, K., and Jow, T. (2003). The low temperature performance of Li-ion batteries. *J. Power Sources* 115, 137–140. doi: 10.1016/S0378-7753(02)00618-3

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest. For full transparency we declare that NS was seconded on a 50% basis to Food Standards Scotland (FSS) as Chief Scientific Adviser during his involvement in this project.