Recording Provenance of Food Delivery Using IoT, Semantics and Business Blockchain Networks

Milan Markovic*, Peter Edwards† and Naomi Jacobs‡
University of Aberdeen, Computing Science, Aberdeen, UK.
Email: *milan.markovic@abdn.ac.uk, †p.edwards@abdn.ac.uk, ‡naomi.jacobs@abdn.ac.uk

***Abstract*—In recent years, the food delivery sector has experienced an influx of disruptive models triggered by advances in sensing, robotics and data science. Inexpensive IoT technologies when combined with a secure and tamperproof data management infrastructure offer a potential solution to issues such as safety of perishable products in transit and monitoring of delivery contractors. In this paper we present a prototype architecture utilising IoT devices for monitoring food deliveries, semantic services for managing and reasoning about provenance compliance records, and private blockchain networks for persistent and secure storage.**

I. Introduction

Last mile food delivery refers to the last leg of the food distribution process from businesses to its final destination (e.g. a restaurant, home, etc.) using diverse modes of transport such as cars, vans and bicycles. If we consider a typical online takeaway delivery scenario, this will involve various stages during which the order is first made available for delivery, then collected by a delivery person, stored in a vehicle, and transported to the customer. During the transport stage, the food leaves the relatively controlled environment of food premises, and can be subject to a number of environmental factors (such as high ambient temperatures, little/no refrigeration) depending on the mode of transport used.

As highlighted in the 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 ...". HACCP[2] is a widely accepted food safety management system used to provide guidance to food businesses on preventing and controlling potential food borne health hazards (e.g. microbiological, chemical or physical). HACCP introduces *critical limits* that food businesses must comply with; for example, if food is to be kept chilled then the temperature of the refrigerator must be no higher than 5°C.

For many small, and medium-sized businesses the cost of modern customised solutions that can monitor delivery processes is prohibitive. Inexpensive IoT technologies combined with a secure and tamperproof data management infrastructure thus offers a potential solution. Existing IoT technologies can be used to monitor locations and temperatures of delivery vehicles as well as individual products - with some businesses already using such solutions to monitor transport of produce. However, such systems are typically deployed for monitoring business operations and customers cannot generally consume this data. In addition, the IoT devices are often used only as connected data loggers and hence are prevented from gaining a broader contextual awareness (e.g. an IoT sensor cannot recognise that it is currently stored in a specific location such as a smart fridge).

The system described in this paper, explores the potential for utilising the increasing computational capabilities of IoT devices to facilitate smart monitoring of food deliveries. IoT devices are tasked with processing of raw temperature data and producing aggregated reports on compliance with food safety constraints during delivery stages. The system's aim is to utilise IoT devices as trusted sources of information about temperature conditions during the delivery process, and to enable them to relay such information directly to the customer at the point of delivery.

The system also utilises semantic provenance annotations to produce machine-readable descriptions of such reports to facilitate seamless integration of the results by other systems. Semantic technologies such as ontologies [1] and linked data [2] have been recognised for their benefits in the context of data integration and automated processing for decision support [3]. In recent years, we have also seen an increasing interest in semantic web technologies in the context of e-Government [4] and Open Government Data [5]. We argue that these technologies could play a key role in food industry scenarios that require data integration from multiple businesses; for example, as part of a compliance monitoring platform for food regulators. In our previous work, we explored the use of the W3C PROV-O ontology [6] for documenting provenance-based compliance records in a commercial kitchen environment. We proposed the FS-PROV extension [7] and a prototype implementation of a stream-based architecture for server-side conversion of raw sensor data described using the SSN ontology [8] into a concise compliance record using provenance abstractions [9]. The work presented in this paper is a continuation of these efforts with a focus on utilising the edge computing paradigm by allowing the IoT devices to assume responsibility for processing of raw sensor data.

Finally, our system stores semantic data using novel technologies for creating business blockchain networks that facilitate a permissioned, auditable and immutable data storage

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

[2]https://www.food.gov.uk/business-guidance/hazard-analysis-and-critical-control-point-haccp

978-1-5386-5541-2/18/$31.00 ©2018 IEEE

layer. Blockchain networks such as IBM Food Trust[3] are part of an emerging trend in the food sector, as the ability to store immutable records detailing transactions between businesses (e.g. placing orders, payment for goods, etc.) enhances transparency and traceability in a food supply chain. Blockchain technology is promoted as a secure, efficient, and decentralised approach to storing and publishing food related data in a heterogeneous environment with multiple stakeholders [10].

II. Application Scenario

The system assumes responsibility for compliance monitoring at the point when food is packed for delivery. A "context-aware" IoT logger is attached to the delivery container and travels with a specific delivery until it reaches the customer. The IoT logger is pre-programmed with an ID identifying the order and is also aware of the different stages of the delivery workflow and associated food safety constraints. For example, after food is packed for delivery it might be placed in cold storage until it is picked up by a delivery driver. Then it is placed in a delivery van and delivered to the customer. The IoT logger interacts with IoT beacons (IR or Bluetooth based) to determine its current location (e.g. in a restaurant fridge, delivery van, etc.).

Based on its current location, the IoT device computes whether any of the food safety constraints relevant for that particular part of the business workflow have been breached. For example, if the device is in the fridge and the air temperature is observed to be above the required threshold for a significant amount of time, the IoT logger records that a compliance constraint has been breached.

At the point of delivery, customers use a mobile app to interact with the IoT logger to access the recorded data. The app is also used to relay the data into a webservice that generates semantic provenance descriptions capturing a compliance record of the delivery. Such records are then stored on the business blockchain network so it can be used by other applications (e.g. a food regulator inspecting business processes).

III. System Requirements

The system requires cooperation between a number of components in order to deliver the in situ sensing capabilities and sufficient computational power to generate semantic descriptions. In addition, additional devices such as beacons and mobile apps are required to aid spatial awareness of the IoT devices and facilitate relay of data to cloud services.

We have derived a number of requirements for the individual system components, which are detailed in the remainder of this section.

1) IoT Logger: A core component of the system is the IoT device that travels with the food order and monitors temperature against the predefined constraints associated with different stages of a business process. The requirements are:

- determine current physical location based on signals received from IoT beacons
- observe and evaluate temperature readings according to the current delivery stage inferred from the detected location
- publish results of compliance monitoring over NFC and Bluetooth

2) Location Beacons: A simple IoT device placed in a fixed location used to aid the IoT logger in terms of determining its current location. The requirements are:

- broadcast an ID of a specific location

3) Server App: This component is responsible for generating semantic provenance compliance records to describe data received from the IoT logger. The requirements are:

- create a semantic representation of the compliance report produced by the IoT logger
- save the semantic representation of the compliance report on the blockchain network

4) Private Blockchain network: Persistent storage and data sharing with third party applications is handled by a private blockchain network. The requirements are:

- define models to represent business entities performing food deliveries, customers, and assets (i.e. deliveries)
- define a model for a delivery transaction which will also contain a compliance record
- define permissions for data access
- provide a RestFul API

5) Phone App: The mobile app provides an interface between the customer and the compliance data generated by the other system components. The requirements are:

- read data from the IoT logger
- upload data for further processing into the server app
- generate customer report based on the received data

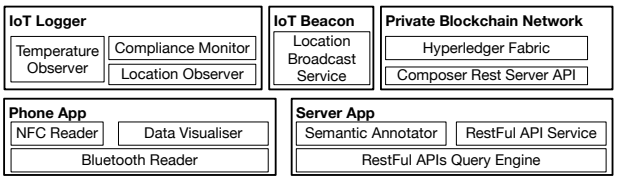

Fig. 1. An overview of system components.

IV. System Architecture

Figure 1 depicts a simplified overview of the implemented system components and their functionality to satisfy the requirements identified in the previous section. The four main functions performed by the system are *compliance monitoring*, *semantic data representation*, *data storage* and *data access*. These are discussed in more detail below. Figure 2 provides an overview of an activity flow within the system including the main messages passed between the components.

A. Compliance Monitoring

The prototype system currently works with Puck.js[4], a device that can measure light and temperature, can control

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

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

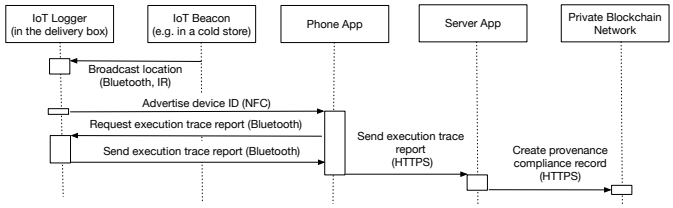

Fig. 2. An activity diagram detailing interactions between system components.

infrared devices, and has a programmable push button. It can also communicate via Bluetooth and NFC. The device cannot access the Internet directly, but it can utilise a proxy device. Therefore, the system utilises a smartphone app, which the end customer uses at the point of delivery to retrieve the results of a delivery assessment performed by the IoT device. The app informs the customer whether relevant HACCP standards have been met, and will also relay the data to the cloud-based infrastructure for storage. The mobile app has been developed using the Apache Cordova framework[5]. Users interact with the Puck.js devices by tapping it with their phones. Data containing the results of temperature monitoring and the location context recorded by the device are transferred to the app via NFC.

B. Semantic Data Representation

The IoT logger determines whether compliance constraints for individual delivery process stages were satisfied. However, due to its limited processing power, generating semantic provenance descriptions is handled by a JAVA-based server app using the Apache Jena framework[6]. The app creates a workflow representation of a delivery plan using the FS-PROV ontology consisting of a series of interconnected steps such as cold storage on premises, cold storage in a van, out of the cold storage. The plan also includes representation of the delivery item and associated constraints (e.g. average air temperature measured over a 10 min period cannot exceed 5°C). The server app receives IoT data relayed by the mobile app through a RestFul API implemented using the Spring Framework[7]. The delivery plan represents information on what was expected to happen during the delivery process. This is linked to the representation of an execution trace, which is created based on the data received from the IoT logger. Such data then includes the record of processes that actually occurred during the delivery and the results of constraint evaluations.

C. Data Storage & Access

The system leverages the Hyperledger Composer project[8] for creating business networks using smart contracts and deploying them on Hyperledger Fabric[9]. Smart contracts consist of a series of models representing a business participant, a delivery and a delivery transaction, their attributes (e.g., business name, order ID, delivery status), data access permissions, and functions that users of the network can use to change the state of the records on the network. The smart contract functions are exposed via a RestFul API using the Composer Rest Server.

[5]https://cordova.apache.org/
[6]https://jena.apache.org/
[7]https://spring.io/
[8]https://hyperledger.github.io/composer/
[9]https://www.hyperledger.org/projects/fabric

V. Conclusions & Future Work

In this paper, we have described a novel prototype system architecture for recording provenance-based semantic descriptions of compliance monitoring during food deliveries using IoT and business blockchain networks.

Our plans for future work involve testing of the proposed architecture in a real-world setting as part of a pilot deployment with food businesses. We also plan to conduct a number of user studies to evaluate user attitudes towards data generated by IoT devices and their ability to understand and interact with such data. We will also interview food regulators to understand the perceived value of having such data available through the means of semantic representation and private blockchain networks.

Acknowledgment

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

References

[1] D. L. McGuinness, F. Van Harmelen *et al.*, "Owl web ontology language overview," *W3C recommendation*, vol. 10, no. 10, p. 2004, 2004.
[2] C. Bizer, T. Heath, and T. Berners-Lee, "Linked data: The story so far," in *Semantic services, interoperability and web applications: emerging concepts*. IGI Global, 2011, pp. 205–227.
[3] E. Blomqvist, "The use of semantic web technologies for decision support–a survey," *Semantic Web*, vol. 5, no. 3, pp. 177–201, 2014.
[4] R. Klischewski, "Semantic e-government," *E-Government: Information, Technology, and Transformation: Information, Technology, and Transformation*, p. 219, 2015.
[5] Y. Charalabidis, C. Alexopoulos, and E. Loukis, "A taxonomy of open government data research areas and topics," *Journal of Organizational Computing and Electronic Commerce*, vol. 26, no. 1-2, pp. 41–63, 2016.
[6] T. Lebo, S. Sahoo, and D. McGuinness, "PROV-O: The PROV ontology," Tech. Rep., April 2013. [Online]. Available: https://www.w3.org/TR/2013/REC-prov-o-20130430/
[7] M. Markovic, P. Edwards, M. Kollingbaum, and A. Rowe, "Modelling provenance of sensor data for food safety compliance checking," in *Provenance and Annotation of Data and Processes*, M. Mattoso and B. Glavic, Eds. Cham: Springer International Publishing, 2016, pp. 134–145.
[8] M. Lefrançois, K. Janowicz, A. Haller, S. Cox, D. L. Phuoc, and K. Taylor, "Semantic sensor network ontology," W3C, W3C Recommendation, Oct. 2017, https://www.w3.org/TR/2017/REC-vocab-ssn-20171019/.
[9] M. Markovic and P. Edwards, "Semantic stream processing for iot devices in the food safety domain," *Proceedings of Semantics 2016*, 2016.
[10] F. Yiannas, "A new era of food transparency powered by blockchain," *Innovations: Technology, Governance, Globalization*, vol. 12, no. 1-2, pp. 46–56, 2018.