Industrial Internet of Things: A Provenance-based Solution for Monitoring Food Products

Sabah Suhail, Shashi Raj Pandey, Choong Seon Hong
Department of Computer Engineering, Kyung Hee University, Yongin, 446-701 Korea
Email: sabah, shashiraj, cshong@khu.ac.kr

Abstract

In the food industry, manufacturing, processing, packaging, and transportation of food products are critical processes as it requires continuous monitoring of the environmental factors (for instance, temperature) that may affect the quality of food. Any deviation in the ambient temperature may make the ingredients or the food items hazardous for consumption. To deal with such situations in the industries, sensors connected to the Internet are collectively characterized as *Industrial Internet of Things* (IIoT). The connected things are responsible for tracking the location of the food item and monitoring quality throughout the process. However, IIoT faces two primary challenges. Firstly, how the information is stored and managed to make it available to all entities involved in the food industry. Secondly, how to track and trace food items as it passes through different processing phases. To answer these questions, we propose an approach to maintain a complete log of sensor data along with complete provenance information. We use IOTA distributed ledger technology (DLT) to share data transparently among all participating entities. We use the Masked Authenticated Messaging (MAM) protocol to provide data confidentially, data integrity, and restricted data accessibility. Finally, we simulate the proposed scheme on the Raspberry PI 3B IoT platform and evaluate its performance in terms of attaching and retrieving sensor data, along with provenance information at different time intervals.

Keywords—DLT, IOTA, IoT, IIoT, Message Authenticated Messaging, sensor, provenance.

I. Introduction

The use of IoT technologies in the industry opens a new paradigm called as Industrial Internet of Things (IIoT) or Industrial Internet [1]. The IoT sensors generate, collect, and process an enormous amount of data, and are able to communicate with other sensors and remote computers. To solve automation challenges in the industrial sector, sensors are deployed to keep track of a variety of activities. For instance, in the food industry, sensors are responsible for controlling and monitoring the quality of food products (e.g., perishable food items). Such monitoring is crucial as they have to maintain the quality of food items and it must comply with HACCP (Hazard Analysis and Critical Control Points) standards. Any negligence to the standards may have disastrous results on the health or even life of consumers.

To facilitate the monitoring of food items, the first challenge is to collect and manage sensor data during the entire cycle of food products. Provenance plays an important role in keeping track of data [5], [6]. Another challenge is to ensure the access rights, security, and availability of data. IOTA is a DLT that is trying to make meaningful inroads into the IIoT world. Though blockchain has been adopted by many organizations, however, the long-run limitations (such as scalability and quantum-resistance) associated with blockchain can not be neglected [2]. IOTA Foundation has introduced MAM protocol that provides data confidentiality, data integrity, and data authentication to ensure reliability of data. Since data is at the crux of IIoT, we adopt IOTA together with the MAM protocol to construct provenance information on a product ledger. The main contributions of the paper are as follows:

- We propose a product ledger that monitors food products based on sensor data. It tracks data related to intermediate entities which are responsible for handling the product throughout the food industry process.
- We use IOTA DLT to keep the shared data accessible to all authorized participating entities, thereby getting rid of incomplete or broken information across multiple resources.
- We use MAM protocol to maintain integrity, authenticity, and confidentiality of the data in the ledger.
- Finally, we simulate the proposed scheme on Raspberry PI 3B which is commonly used as a hardware IoT platform.

The paper is organized as follows. Section II presents the preliminaries of IOTA and MAM protocol. Section III discusses the system model. Section IV explains the working of the provenance scheme. Section V presents the experimental results. Finally, in Section VI we conclude the paper with our future goals.

II. Background

A. IOTA

IOTA is a distributed ledger based on a directed acyclic graph (DAG) structure called Tangle which enables the storage and retrieval of data by the participating entities in the network [3]. IOTA plays a significant role in the Machine-to-Machine (M2M) or Machine-to-Human (M2H) economy. The striking features of IOTA including scalability, feeless transactions, quantum-resistant, and off-line transactions make it an ideal candidate for the IoT world in contrast to the blockchain.

B. Masked Authenticated Messaging (MAM)

To ensure data integrity, data confidentiality, and fine-grained data access control, IOTA introduces Masked Authen-

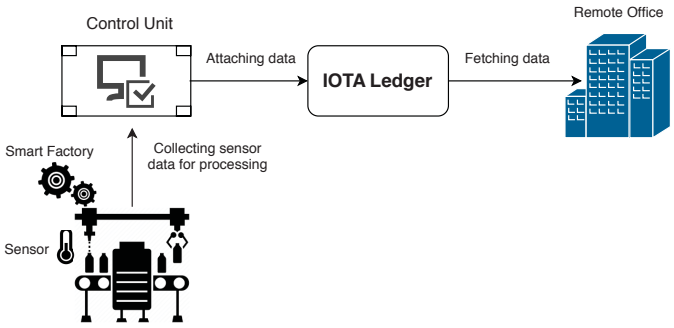

Fig. 1: Illustration of smart food factory collecting, attaching, and fetching of sensor data.

ticated Messaging (MAM) protocol. In MAM, each participating entity publish its data via a channel. Any interested candidate can access the data upon the channel subscription. Due to space limitation, we refer to [4] for further details on MAM.

III. System Model

A. Network Model

The network model consists of the connected entities involved in the industrial automation process (e.g., manufacturing, processing, production), for instance, sensors (humidity, temperature, optical, infrared, image, proximity). In our case of food monitoring, we particularly consider sensors (DHT-11) for monitoring temperature and humidity.

B. Data Model

The data model consists of two types of information: (i) sensor data (S_d), and (ii) provenance information (P_{info}) as shown in 1. S_d contains information related to temperature ($temperature_r$) and humidity ($humidity_r$) data values along with timestamp (t_s), whereas P_{info} contains auxiliary information related to batch or package holding items. Currently, we consider temperature and humidity sensor data values. However, data from other sensors (for instance, pressure, motion, and acceleration) can be incorporated in the similar way. The purpose of including P_{info} along with S_d is to extract the relevant ordered details about the underlying processes, for example, S_d is retrieved from which batch or package IDs accordingly at each intermediate phase. Furthermore, P_{info} may contain information about granular details if multiple processes are taking places in parallel. For example, a machine ID *M101* operating at unit *A* situated at location *L*. However, for the sake of simplicity we only consider that a process is taking place at a single unit. We consider two primary entities including data publisher (d_p) and data receiver (d_r) such that the d_p can publish (or attach) the data to tangle while d_r can receive (or fetch) data from tangle. The data model can be represented as follows:

$$Data \leftarrow S_d||P_{info}, \tag{1a}$$

$$S_d \leftarrow t_s||temperature_v||humidity_v, \tag{1b}$$

$$P_{info} \leftarrow batch_{ID}||package_{ID}. \tag{1c}$$

Therefore, both sensor data and provenance data are necessary to provide a complete information about any process, i.e., the sensor data provides information about the quality of food item whereas the provenance data provides information about each intermediate entity involved in the processing.

IV. Provenance Scheme

A. Attaching Data to Tangle

In order to attach sensory data to the Tangle, the data publishers d_p (for instance, a DHT-11 sensor) publishes the data (including S_d and P_{info}) on its channel. To generate sample sensor data, we use DHT-11 sensor that records temperature and humidity readings at a time interval of one minute. It is important to mention that the time interval can be customized depending on the application requirement, or we can employ channel splitting that allows data publishers to divide the channel data into subsets of data. Such feature can facilitate the monitoring of the sensor data at more granular sub-intervals to observe data anomaly whenever required. In addition to S_d, we also include provenance information P_{info} associated with S_d. In our case, we assume that sensors are affixed with a batch or a package and are responsible for food monitoring during processing or packaging. As sensor data is vulnerable to data forging and false data injection, therefore, we employ MAM protocol to enforce data confidentiality, data integrity, and restricted data accessibility. We use a restricted channel mode of MAM protocol that allows only authorized parties to access and then decrypt the data by using a shared secret key (K_s).

B. Fetching Data from Tangle

In order to fetch data from Tangle, the data receiver d_r (for instance, control unit) subscribe to the channel of the data publisher. Secondly, d_r uses Merkle root value to fetch the required or complete log of data. Thirdly, d_r decrypt the data by using the shared secret key (K_s). Finally, S_d and P_{info} are extracted from data to analyze the readings and other associated details. It is important to note that the data can be fetched either by the control unit or by any other authorized entity monitoring the workflow of that particular unit or process.

V. Simulation

In order to simulate the proposed scheme, we use Raspberry PI 3B as a hardware platform for IoT. The hardware specifications of Raspberry PI 3B are shown in Table I. Considering the

TABLE I: Specifications of Raspberry Pi 3B hardware platform.

Platform name	CPU	CPU core	RAM size	Power consumption	Number of cores
Raspberry Pi 3B	BCM2837	Cortex-A53	4	1 GB	221.0 mW per core

(a) (b)

Fig. 2: (a) Attaching payload to Tangle, (b) fetching payload from Tangle.

resource-constrained nature of IoT devices, we use Raspberry PI 3B as a light node that relie on IOTA full node to do proof of work (POW) on its behalf. We run our simulation for varying payload size, whereas the time interval for recording sensors values is set to 1 minute. Fig. 2a and Fig. 2b show the time required to attach and fetch data (including S_d and P_{info}) for payload size (100, 500, 1000) respectively. It can be observed that process of attaching and fetching sensor data is independent of time. Furthermore, we also measure the CPU and memory usage for attaching and fetching data to the Tangle (shown in Fig. 3). It is observed that more CPU and memory consumption is required during the fetching phase as compared to the attaching phase. This is because the fetching process is performed locally while the attaching process relies on remote node to do further processing. Moreover, CPU and memory consumption is also independent of payload size.

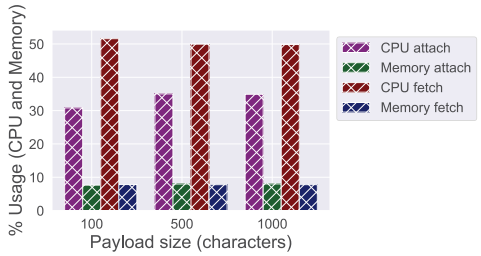

Fig. 3: CPU and memory usage.

VI. Conclusion

In this paper, we presented a provenance-based system for IIoT that is capable of monitoring, recording, and retrieving of sensor data during food processing or packaging. We use IOTA ledger to store and retrieve sensor readings. In addition, we also trace the product processing stages as it passes through various phases, and store it as provenance information. This collective holistic view of sensor data and provenance information can enable the food quality monitoring teams to analyze and adjust the ideal environment conditions for the food items. Keeping in mind the importance of trustworthy data, we make use of the MAM protocol to ensure the integrity and accessibility of data. We are planning to apply track and trace provenance-based solution to solve the other challenging issues in Industry 4.0, for example, counterfeit problem as a part of our future work.

Acknowledgment

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (No.2015-0-00557, Resilient/Fault-Tolerant Autonomic Networking Based on Physicality, Relationship and Service Semantic of IoT Devices). *Dr. CS Hong is the corresponding author.

References

[1] Boyes, Hugh, et al. The industrial internet of things (IIoT): An analysis framework. *Computers in Industry*, 101:1–12, 2018.

[2] Sabah Suhail, et al. Orchestrating product provenance story: When IOTA ecosystem meets the electronics supply chain space. *arXiv preprint arXiv:1902.04314*, 2019.

[3] S Popov. The tangle. white paper. *Available at: Iota. org*, 2016.

[4] ABmushi. Iota: Mam eloquently explained. Available at: https://medium.com/coinmonks/iota-mam-eloquently-explained-d7505863b413 (Accessed 30 September 2019).

[5] Sabah Suhail, et al. Provenance-enabled packet path tracing in the RPL-based Internet of Things. *arXiv preprint arXiv:1811.06143*, 2018.

[6] Faheem Zafar, et. al. Trustworthy data: A survey, taxonomy and future trends of secure provenance schemes. *Journal of Network and Computer Applications*, 94:50–68, 2017.