A Provenance-based Solution for Tracking Sensor Data in the Pharmaceutical Supply Chain

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 pharmaceutical supply chain (PSC), the process of transporting medicines is a critical process as it requires continuous monitoring of temperature-controlled products. Any deviation in the temperature may make the medicine or vaccination hazardous for consumption by patients. Hence, a tracking solution is required that enables the participating entities in the PSC to acquire information about medicines condition during transportation. In this regard, provenance plays a key role in maintaining lineage information about product phases as it evolves throughout the supply chain (SC). In this paper, we propose a provenance-based solution to maintain and monitor a complete log of sensor data along with supporting provenance information whenever required. We use IOTA distributed ledger technology (DLT) to share data transparently among all participating entities. Furthermore, we use the Masked Authenticated Messaging (MAM) protocol to facilitate data confidentially, data integrity, and restricted data accessibility. Finally, we evaluate the proposed approach in terms of attaching and retrieving sensor data along with provenance information at different time intervals.

Keywords—DLT, IOTA, IoT, Message Authenticated Messaging, sensor, supply chain, provenance

I. Introduction

A pharmaceutical supply chain (PSC) involves a complex and sophisticated process during which the multiple participating supply chain (SC) entities interact with each other to produce and deliver medicines and vaccinations to the pharmacies. The crucial step during the production process of drugs is to ensure the safe delivery of pharmaceutical drugs in order to assure its usability. For instance, in August 2017 a shipment from a single lot of Intralipid 20% IV fat emulsion, 100 mL bags (Baxter International, Inc.), was improperly exposed to subfreezing temperatures during transit to a distribution facility[1]. As temperature-sensitive medicinal products travel across the globe, many external conditions specifically temperature, humidity, and light can reduce their efficacy and quality. Hence, in order to maintain desired temperature ranges and also to fulfill regulatory compliance (for instance, Good Distribution Practice (GDP) and Food and Drug Administration (FDA)), a monitoring solution is required.

In a temperature-controlled supply chain (also referred to as *cold chain*), the medicines are need to be stored at three categories of temperature including (i) cold (-20°C), (ii) cool (2°– 8°C), and (iii) ambient (15°– 25°C). However, every medicine has a *stability data* which describes the life of a medicine for a period of time X under certain temperature range Y [1]. During transportation or logistics, if the temperature and other conditions deviate significantly from the standard requirements, the sender and the receiver are notified of the divergence. Therefore, upholding quality standards is a challenging task in the PSC that involves monitoring, recording, and analyzing environmental variations from manufacturer's point of origin to the point of end users.

Considering the process of transporting medicines under critical conditions require a provenance-based trace and track solution that is able to notify alerts to the participating entities in the PSC about the current status of drugs on the go. Provenance plays a key role in gathering and maintaining lineage information about a product by tracking information about the source and intermediate phases acted upon a product [2]–[5]. To do so, the monitoring data collected from the sensors affixed with the medicine containers or batches are stored by DLT called IOTA. The distributed IOTA ledger only allows the legitimate participating entities to attach and fetch sensor data at one place, thereby solving the problems of unreliable and scattered information [6]. Thus, IOTA can be used to monitor sensor data efficiently and effectively.

The main contributions of the paper are as follows.

- We propose a product-specific monitoring ledger that trace and track product journey data throughout the supply chain process.
- We use IOTA DLT to keep the shared data accessible to all authorized participating entities, thereby getting rid of fragmented information across multiple databases.
- We use MAM protocol of IOTA to maintain the integrity, authenticity, and confidentiality of the data in the product ledger.

The rest of the paper is organized as follows: Section II presents the supply chain overview. Section III discusses the system model including network, provenance and attacker models. Section IV explains the working of the provenance scheme. Section V presents the experimental evaluation results. Finally, we conclude the paper with future research directions in Section VI.

[1]https://www.baxter.com/baxter-newsroom/baxter-initiates-voluntary-nationwide-recall-one-shipment-intralipid-20-iv-fat

Fig. 1: Pharmaceutical Supply Chain (PSC) showing primary participating entities.

II. Background

A. IOTA

IOTA is a revolutionary distributed ledger which utilizes a directed acyclic graph (DAG) structure called Tangle to store and retrieve data by the peers participating in the network [7]. IOTA is specifically developed for Internet of Things (IoT) or Machine-to-Machine (M2M) economy. IoT devices will generate a huge amount of data which can be stored on the Tangle.

B. Masked Authenticated Messaging (MAM)

IOTA employs Masked Authenticated Messaging (MAM) protocol to ensure data integrity, data confidentiality, and fine-grained data access control. In MAM, each SC entity owns a channel through which it can publish its data whereas the interested parties can access the data upon channel subscription. Due to space limitation, we refer to our paper [6] for more details on IOTA DLT and MAM.

III. System Model

In this section, we discuss network, data, and provenance model of our proposed scheme.

A. Network Model

The network model consists of the primary participating entities of a SC process, for instance, raw material suppliers, manufacturers, logistics, and pharmacies (as shown in Fig. 1).

B. Data Model

The data model consists of sensor data (S_d) along with timestamps (T_s). We only consider temperature sensor data. However, other sensors data (for instance, humidity, light, and location information) can be incorporated in the same way.

C. Provenance Model

The provenance information (P_{info}) comprise of supporting information along with S_d , for instance, batch ID ($Batch_{ID}$) and cargo ID ($Cargo_{ID}$). The purpose of including P_{info} along with S_d is to track and associate S_d with further details, for example, S_d is retrieved from which batch and cargo IDs accordingly.

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

$$S_d \leftarrow T_s, \tag{1b}$$

$$P_{info} \leftarrow Cargo_{ID}||Batch_{ID}. \tag{1c}$$

As we are only tracking sensor data, hence, our P_{info} is limited. However, we will include other supporting information for tracing purposes as a part of our future work.

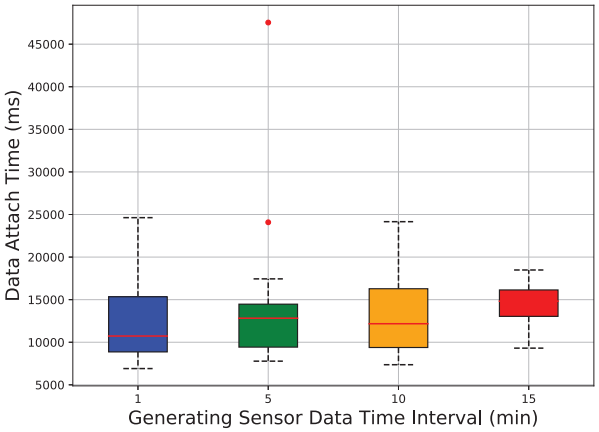


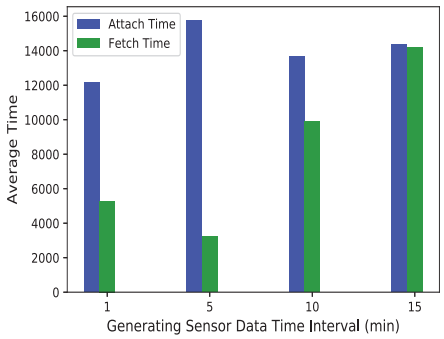
Fig. 2: Average time (msec) required to attach data to the Tangle.

IV. Provenance Scheme

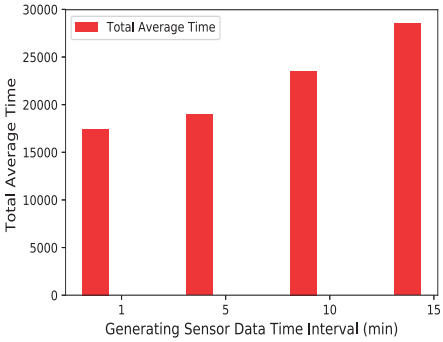
A. Attaching Provenance Data to the Tangle

In order to attach the data to the Tangle, the data publishers P (for instance, supplier) publishes the sensor data (S_d) on its channel. We generate random temperature data at different time intervals. In addition to S_d, we also include provenance information P_{info} associated with S_d. As sensor data is vulnerable to data forging and data injection, therefore, we employ MAM protocol to enforce data confidentiality, data integrity, and restricted data accessibility. To do so, 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) upon retrieval.

Another important feature is *Channel Splitting* that allows data publishers to divide the channel data into subsets of data. Such property can be used to monitor the sensor data at more granular sub-intervals to observe data anomaly whenever required. We discuss channel splitting in our paper [6].



(a) Comparison between attaching and fetching time.



(b) Total average time to attach and fetch data.

Fig. 3: Attaching payload data to Tangle and fetching payload from Tangle.

B. Fetching Provenance Data to the Tangle

In order to fetch data from Tangle, firstly, the data receiver R (for instance, buyer) subscribe to the channel of data publisher. Secondly, R uses Merkle root value to fetch the required or complete log of sensor data S_d. Thirdly, R decrypt the data and P_{info} by using the shared secret key (K_s).

V. Simulation

We run our simulation for an average time of 1 hour by varying time interval from 1 minute to 15 minutes. Fig. 2 shows the minimum, first quartile, median, third quartile, maximum, and outliers for different sensor data intervals. The average time required to attach data to the Tangle and fetch data from the Tangle is shown in Fig. 3a. It can be observed that the attaching and fetching sensor data is independent of time. Also, the total average time is shown in Fig. 3b. It is important to note that sensor data also includes supporting provenance information during attaching and fetching phases of sensor data to the Tangle.

VI. Conclusion

In this paper, we presented a provenance-based system that enables the participating entities of a pharmaceutical supply chain to monitor the sensor data during transportation of medicines. We use IOTA ledger to allow the SC entities to access the distributed data transparently. Furthermore, we use MAM protocol to ensure the integrity and accessibility of data. We are planning to apply track and trace provenance-based solution to solve the pharmaceutical counterfeit problem as a part of our future work.

Acknowledgment

This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the Grand Information Technology Research Center support program (IITP-2018-2015-0-00742) supervised by the IITP(Institute for Information & communications Technology Promotion). *Dr. CS Hong is the corresponding author.

References

[1] https://bitcoinmagazine.com/articles/modum-io-s-tempurature-tracking-blockchain-solution-wins-accolades-at-kickstarter-accelerator-1479162773/.

[2] Sabah Suhail, Choong Seon Hong, M Ali Lodhi, Faheem Zafar, Abid Khan, and Faisal Bashir. Data trustworthiness in iot. In *Information Networking (ICOIN), 2018 International Conference on*, pages 414–419. IEEE, 2018.

[3] Sabah Suhail, Choon Seong Hong, Zuhaib Uddin Ahmad, Faheem Zafar, and Abid Khan. Introducing secure provenance in iot: Requirements and challenges. In *Secure Internet of Things (SIoT), 2016 International Workshop on*, pages 39–46. IEEE, 2016.

[4] Sabah Suhail, Muhammad Abdellatif, Shashi Raj Pandey, Abid Khan, and Choong Seon Hong. Provenance-enabled packet path tracing in the rpl-based internet of things. *arXiv preprint arXiv:1811.06143*, 2018.

[5] Faheem Zafar, Abid Khan, Saba Suhail, Idrees Ahmed, Khizar Hameed, Hayat Mohammad Khan, Farhana Jabeen, and Adeel Anjum. Trustworthy data: A survey, taxonomy and future trends of secure provenance schemes. *Journal of Network and Computer Applications*, 94:50–68, 2017.

[6] Sabah Suhail, Choong Seon Hong, and Abid Khan. Orchestrating product provenance story: When iota ecosystem meets the electronics supply chain space. *arXiv preprint arXiv:1902.04314*, 2019.

[7] Sergei Popov. Iota whitepaper. *Technical White Paper, year*, 2017.