Track and Trace Solutions to Combat Counterfeiting in Healthcare 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 healthcare supply chain, manufacturing, processing, packaging, and transportation of medical equipment are critical processes as it requires (i) continuous monitoring of the environmental factors (for instance, temperature, humidity, pressure) that may affect the quality of sensitive healthcare equipment or pharmaceuticals and (ii) tracking of equipment to thwart counterfeiting during various supply chain processes. To automate the monitoring and tracking processes, sensors play a significant role in the Industrial Internet of Things (IIoT). However, IIoT faces two main challenges. Firstly, how to store and manage the information in a distributed and decentralized way thereby making it available to all participating entities in the healthcare supply chain. Secondly, how to trace back the origin of healthcare equipment as it passes through different supply chain phases. In this paper, we propose a provenance-based approach to maintain comprehensive information about the healthcare equipment staring from its manufacturing phase until its distribution phase. To solve the aforementioned challenges, we use IOTA distributed ledger technology (DLT) to achieve distributed and decentralized data among all participating entities. We use the Masked Authenticated Messaging (MAM) protocol to facilitate data confidentially, data integrity, and data accessibility. Finally, we simulate the proposed scheme on the Raspberry PI 3B IoT platform and evaluate its performance in terms of latency and energy consumption during attaching and fetching data, along with provenance information at different time intervals.

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

I. Introduction

The healthcare supply chain deals with the production of healthcare equipment (such as diagnostic equipment, treatment equipment, life-supporting equipment, medical laboratory equipment, etc.). Such production processes in the supply chain involve various complex sub-processes such as manufacturing, processing, and distribution of medical equipment across the globe. To facilitate automated processing in the supply chain the use of Internet of Things (IoT) technologies in Industry 4.0 referred to as the Industrial Internet of Things (IIoT) or Industrial Internet is playing a significant role [1]. Instead of manually monitoring or recording the supply chain activities, the IoT sensors collect, process, and analyze data with little human intervention. The deployed sensors are able to keep track of a variety of activities. For example, in the healthcare supply chain, (i) sensors control and monitor the quality of medical equipment during manufacturing, processing, or even transporting of equipment across the globe; (ii) sensors record the underlying operations during the supply chain processes; (iii) sensors log the participants that transport the equipment (its parts or component).

Despite the automation supported by the use of sensors in the supply chain, the healthcare supply chain is facing various ongoing challenges. The first challenge is *how to efficiently collect and effectively manage sensor data* during the entire production cycle. The second challenge is *how to ensure the access rights, security, and availability of data* among the legitimate participating entities. The third challenge is *how to resolve counterfeit issues*, particularly that arise during the pandemic of coronavirus (COVID-19). During COVID-19, due to a huge gap between supply and demand for medical equipment, there is a sharp rise in counterfeit production. Therefore, ensuring the reliability of personal protective equipment (such as test kits for COVID-19 and ventilators) or other epidemic prevention materials (such as masks, gloves, and other protective gear) is of critical concern.

We adopt the following solutions to solve the above-mentioned challenges. Firstly, to facilitate medical materials supply chain tracking, we introduce a provenance-based solution. *Provenance* is used to keep track of the actors and the activities involved in an underlying process [2], [3]. Secondly, we adopt a DAG-structured blockchain called *IOTA* [4] for distributed data storage. Though blockchain DLT has been adopted by many organizations, however, we can not ignore the limitations (such as scalability and quantum-resistance) associated with blockchain [5], [6]. Thirdly, we use the *Masked Authentication Messaging* (MAM) protocol that ensures the reliability of data.

The main contributions of the paper are as follows.

- To resolve counterfeit issues, we propose an *equipment-specific ledger* that trace and track product-related data throughout the healthcare supply chain processes.
- In contrast to the chained-structured blockchain, we selected one of the *DAG-structured blockchains* called *IOTA* to keep the shared data accessible to all authorized participating entities while satisfying other constraints such as scalability.
- To ensure data trustworthiness, we deploy the MAM protocol of IOTA to maintain the integrity, authenticity, and confidentiality of the data in the healthcare equipment ledger.

The rest of the paper is organized as follows: Section II discusses the system model through network, provenance, and

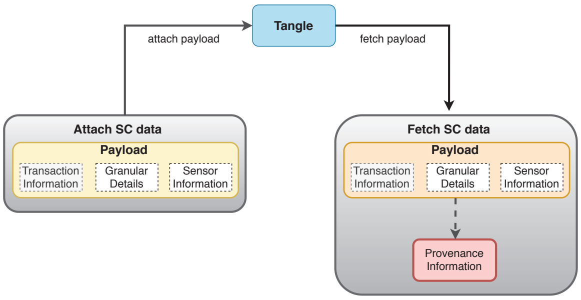

Fig. 1. System model illustrating the process of attaching data to the Tangle, fetching data from the Tangle, and constructing provenance information.

attacker models. Section III elaborates on the working of the provenance scheme in the health care supply chain. Section IV evaluates the proposed provenance-based scheme. Finally, Section V concludes the paper with future work.

II. System Model

In the following section, we discuss the primary components of the network, data, and provenance model of the proposed scheme for the health care supply chain.

A. Network Model

Our network model consists of typical participating entities of a supply chain process, for instance, raw material suppliers, manufacturers, logistics, and warehouses, pharmacies, etc. We also consider sensors that are affixed with medical equipment or batches.

B. Data Model

Our data model consists of sensor ID (S_{id}) collecting sensor data (S_d) where sensors can be attached with the equipment or batches of equipment contained in a cargo. The sensor's data may hold environment-specific data (for instance, temperature, humidity, light) and tracking-based data (for instance location information). S_d also contain other auxiliary information such as timestamps (T_s). Each equipment contained in the batch carried out by a cargo is assigned an equipment ID (E_{id}), batch ID ($Batch_{id}$), and Cargo ID $Cargo_{id}$ respectively. Furthermore, other granular details ($G_{details}$) such as quality (warranty, ISO certification), quantity, price, etc. can be maintained. All of the above-mentioned information is referred to as transaction information (T_{info}) and can be retrieved through transaction ID (T_{id}).

C. Provenance Model

The provenance information (P_{info}) comprise of a comprehensive information including T_{info} (such as E_{id}, $Batch_{id}$, $Cargo_{id}$), additional information ($G_{details}$), and sensor-related information (such as S_{id}, S_d, T_s). The purpose of deriving P_{info} from other details such as (T_{info}, $G_{details}$, S_d) is to track and associate the complete lineage of medical equipments, for example, an equipment is retrieved from *which* batch or cargo under *what* conditions. P_{info} can be extracted as represented in equation 1d where $G_{details}$ can also be fetched upon user request.

$$Data \leftarrow T_{info}||S_d||G_{details}, \tag{1a}$$

$$T_{info} \leftarrow T_{id}||E_{id}||Batch_{id}||Cargo_{id}, \tag{1b}$$

$$S_d \leftarrow S_{id}||T_s, \tag{1c}$$

$$P_{info} \leftarrow T_{id}||S_{id}||E_{id}. \tag{1d}$$

III. Provenance Scheme for Healthcare Supply Chain

A. Process of Attaching Data to the Tangle

To attach data to the Tangle, a data publisher (for instance, a supply chain entity such as manufacturers) publishes the data (including T_{info}, $G_{details}$, and S_d) on its channel. We assume that sensors are attached to medical equipment or batch/package and are responsible for monitoring both location-related and environment-related information. Considering the fact that data (including the sensor data) is vulnerable to attacks (such as data forging and false data injection), therefore, we employ MAM protocol to enforce data confidentiality, data integrity, and restricted data accessibility. In our case, we use a restricted channel mode of MAM protocol that only permits authorized supply chain parties to access and then decrypt the data through a shared secret key.

B. Process of Fetching Data from the Tangle

To fetch data from the Tangle, the data receiver (for instance, a supply chain entity such as hospitals or pharmacies) subscribe to the channel of the data publisher to fetch the required or complete log of data. Upon data decryption by using a secret key, P_{info} is extracted from data to analyze the complete tracking information about medical equipment, sensor readings, and other associated details depending on the user query. Note that the data can be retrieved either by the control unit or by any other authorized entity monitoring the workflow of that particular unit or process.

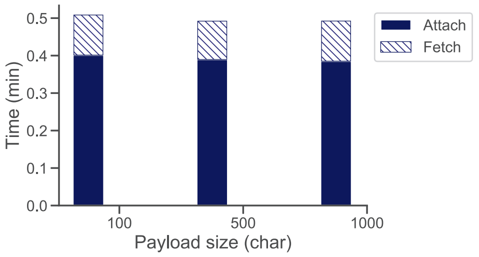

Fig. 2. Average time required to attach data to the Tangle and fetch data from the Tangle.

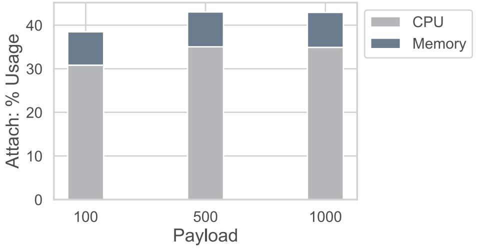

Fig. 3. CPU and memory usage by Raspberry PI 3B during attaching payload to the Tangle.

IV. Simulation

To simulate the provenance-based healthcare supply chain scheme, we use Raspberry PI 3B as a hardware platform for IoT. For demonstrating the process of attaching and fetching sensory data, we affix the DHT-11 sensor with Raspberry PI 3B. However, any other scenario-specific sensor can be deployed to acquire the supply chain data. DHT-11 sensor records temperature and humidity readings as a sample data at a time interval of one minute. Note that the time interval can be customized depending on the application requirement. Furthermore, we can employ a channel splitting feature that allows data publishers to divide the channel data into subsets of data. Thus, monitoring the sensory data at more granular intervals helps to figure out data anomaly. Since IoT devices are resource-constrained therefore, we use Raspberry PI 3B as a light node that utilizes IOTA full node to do the proof of work (POW) on its behalf. We run our simulation for varying payload size. We set the time interval for recording sensor values to 1 minute. Fig. 2 shows the time required to attach and fetch data (including T_{info}, $G_{details}$, and S_d) for payload size varying as 100, 500, 1000. We observed that process of attaching and fetching sensor data is independent of time and payload size. We also measure the CPU and memory usage for attaching data to the Tangle (as shown in Fig. 3) and fetching data to the Tangle (as shown in Fig. 4). By comparing the results, we notice that more CPU and memory consumption is required during the fetching phase in comparison to the attaching phase. Because the process of fetching data is performed locally whereas the attaching process relies on the remote node to do further processing. We also observe that CPU and memory consumption is independent of payload size.

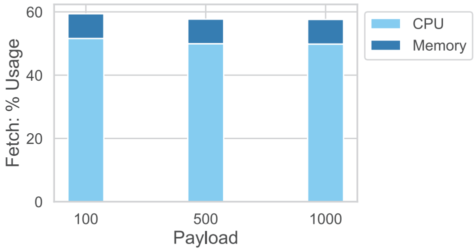

Fig. 4. CPU and memory usage by Raspberry PI 3B during fetching payload from the Tangle.

V. Conclusion

In this paper, we presented a provenance-based system for the healthcare supply chain that is capable of monitoring, recording, and retrieving supply chain data during manufacturing, processing, or delivering medical equipment. We use DAG-based blockchain i.e., IOTA to store and retrieve supply chain data transparently. Furthermore, we construct provenance information by fetching payload to resolve counterfeiting and equipment quality monitoring issues as the healthcare equipment passes through various supply chain phases. We make use of the MAM protocol to ensure the integrity and accessibility of data. In the future, we are planning to extend our provenance-based solution to solve the other challenging issues in the supply chain, for instance, cross-border payments and energy-efficient strategies for resource-constrained IoT.

Acknowledgment

This work was supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT)(2020-0-00364, Development of Neural Processing Unit and Application systems for enhancing AI based automobile communication technology). *Dr CS Hong is the corresponding author.

References

[1] Sabah Suhail, Shashi Raj Pandey, and Choong Seon Hong. Industrial internet of things: A provenance-based solution for monitoring food products.

[2] Sabah Suhail, Rasheed Hussain, Mohammad Abdellatif, Shashi Raj Pandey, Abid Khan, and Choong Seon Hong. Provenance-enabled packet path tracing in the rpl-based internet of things. *Computer Networks*, page 107189, 2020.

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

[5] 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.

[6] Sabah Suhail, Rasheed Hussain, Abid Khan, and Choong Seon Hong. On the role of hash-based signatures in quantum-safe internet of things: Current solutions and future directions. *arXiv preprint arXiv:2004.10435*, 2020.