Data Reselling in IoT Data Marketplace

Pooja Gupta
Computer Science
UNSW Sydney
pooja.gupta@unsw.edu.au

Volkan Dedeoglu
CSIRO, Data61
Brisbane
volkan.dedeoglu@data61.csrio.au

Salil S. Kanhere
Computer Science
UNSW Sydney
salil.kanhere@unsw.edu.au

Raja Jurdak
Computer Science
QUT Brisbane
r.jurdak@qut.edu.au

ABSTRACT

Blockchain-based decentralized data marketplace has gained popularity enabling individuals to share their IoT data in privacy-protective manner. However, current marketplace frameworks lack mechanisms to detect the re-distribution of traded data. This work proposes an IoT data marketplace framework to detect the reselling of data by leveraging the power of smart contracts.

KEYWORDS

IoT, Blockchain, Data Marketplace, watermarking

1 Introduction

IoT generated data such as location, health, sensor data are highly sensitive and reveals personal information. Therefore, the consent of an individual for the use, collection, or distribution of data is essential. Recently, data marketplaces have emerged to facilitate data sharing between a data seller and a data buyer. Blockchain-based data marketplace frameworks democratize data trading by enabling user-controlled data sharing. However, having control over data cannot solve the privacy breach problems, as once the data owner sells the data to a buyer, the buyer can resell the sensitive data to other interested parties.

While related works have considerably explored the copyright protection scheme [1], data right management [2] and data provenance [4], the detection of reselling of data is under-explored. The main aim of this poster is to detect reselling of data in the marketplace by an authorized reseller and ensure fair payment sharing among the data generator or resellers based on the trade agreement.

2 Preliminary Framework

Our framework consists of two major components: 1) watermarking module for embedding, detecting and extracting watermarks [3] in the IoT generated data and 2) two smart contracts: a) trade tracker contract that manages the trade trail and b) marketplace contract for handling agreement and payment settlement. The data reselling detection scheme is illustrated in fig. 1. Data owner or data originator is interested in selling his IoT generated data. He proves his ownership using the Physical unclonable functions challenge-response validation algorithm proposed in [4] and records the data origin in the ledger using the trade tracker contract's *record_trade()*. The genesis record in the trade trail can only be created by the data originator. Trade trail is in the form of a tree structure with nodes as the seller/reseller identifier and edge weight is the payment share. Each trade trail is identified using a unique identifier *(TID)*. Once an agreement is made between buyer and seller, agreement details are recorded in the blockchain using the marketplace smart contract's *agreement()*. Before the data (*D*) is transmitted to the buyer, *Hash(TID)* is embedded in the data (D_w) using the watermarking module. When a reseller resells the purchased data (D_w) to another buyer, the watermark module detects and extracts the watermark *Hash(TID)* before the transmission of the data. Trade tracker contract verifies *Hash(TID)* with the trade trail stored in the ledger using *verify_trade()* and returns the previous buyer list along with their agreed payment share to the *settlement()* of marketplace contract. The marketplace contract performs the fair distribution of the payment among all the data resellers using *settlement()*.

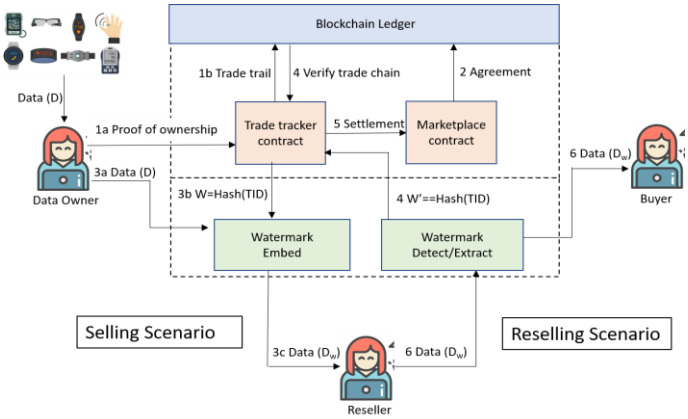

Figure 1: Reselling detection scheme

3 Conclusion

The novel reselling detection scheme is generically applicable across different domains. In our extended work, we demonstrate the detection of data reselling across systems using digital notary who will provide the certificate of authentication and verifies the origin of the data. We will also evaluate the retrieval time and space requirement of trade trail stored in blockchain.

REFERENCES

[1] Meng, Zhaoxiong, et al. "Design scheme of copyright management system based on digital watermarking and blockchain." IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC). Vol. 2. IEEE, 2018.

[2] Ma, Zhaofeng, et al. "Blockchain for digital rights management." Future Generation Computer Systems 89 (2018): 746-764.

[3] Zhang, Guoyin, et al. "A new digital watermarking method for data integrity protection in the perception layer of IoT." *Security and Communication Networks* 2017 (2017).

[4] Javaid, Uzair, Muhammad Naveed Aman, and Biplab Sikdar. "Blockpro: Blockchain based data provenance and integrity for secure iot environments." Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems. 2018.