BEI-TAB: Enabling Secure and Distributed Airport Baggage Tracking with Hybrid Blockchain-Edge System

Fei Wang, Pengbo Si, Enchang Sun, Yuzhao Su
Faculty of Information Technology
Beijing University of Technology
Beijing, China
17865513651@163.com, {sipengbo, ecsun}@bjut.edu.cn, 949634274@qq.com

Abstract—Global air transport carries about 7.3 billion pieces of luggage each year and up to 56 percent of travelers prefer obtaining real-time baggage tracking information throughout their trip. However, the traditional baggage tracking scheme is generally based on optical scanning and centralized storage systems, which suffers from low efficiency and information leakage. In this paper, a blockchain and edge computing based IoT system for tracking of airport baggage (BEI-TAB) is proposed. Through the combination of radio frequency identification technology (RFID) and blockchain, real-time baggage processing information is automatically stored in blockchain. In addition, we deploy Interplanetary File System (IPFS) at edge nodes with ciphertext policy attribute-based encryption (CP-ABE) to store basic baggage information. Only hash values returned by the IPFS network are kept in blockchain, enhancing the scalability of the system. Furthermore, a multi-channel scheme is designed to realize the physical isolation of data, and to rapidly process multiple types of data and business requirements in parallel. To the best of our knowledge, it is the first architecture that integrates RFID, IPFS, CP-ABE with blockchain technologies to facilitate secure, decentralized, and real-time characteristics for storing and sharing data for baggage tracking. We have deployed a testbed with both software and hardware to evaluate the proposed system, considering the performances of transaction processing time and speed.

Index Terms—Blockchain, baggage tracking, RFID, IPFS, edge storage, Attribute-based Access Control

I. INTRODUCTION

According to the latest data from the International Air Transport Association (IATA), global air transport carries about 7.3 billion pieces of baggage every year. The annual increasing number of baggage brings new challenges to airports. The current status and problems in baggage tracking are as follows:

- Optical scanning code is widely used for baggage tracking which leads to the inability to collect real-time information of baggage handling causing passengers’ anxiety for waiting and management’s failure to grasp the handling situation of baggage.
- The lack of unitive platform that managed and shared processing information for each luggage leads to information islands.
- The current logistics records are recorded in centralized database, which more likely leads to passenger information leakage and tampering.
- The huge amount of information poses a challenge to the scalability of the blockchain system.

Compared with optical scanning code, RFID possesses advantages of fast recognition speed, large data capacity, long service life and reusability. Baggage tracking technology based on RFID is one of the most advanced technologies in international baggage management, but the sharing pattern and security of data still need to be promoted[1].

Consortium blockchain only supports the access of the nodes participating in maintenance, and participating nodes need authorization before joining and maintaining blockchain. In addition, its authorized access features can reduce the degree of data leakage, thus enhancing the privacy security of data. Consortium blockchain can guarantee the security of data, but its scalability is challenged in face of hundreds of millions of luggage[2].

IPFS provides a point-to-point (P2P) distributed storage structure, which can easily store a large number of passenger data. IPFS is a content-addressed block storage system with features such as secure transaction hash mapping, high throughput and concurrent access to transactions by peers in the network[3]. Besides, we take advantage of CP-ABE to realize attribute-based access control.

Aiming at the above problems, we propose a blockchain and edge computing based IoT system for tracking of airport baggage (BEI-TAB). Our contributions are mainly as follows:

- The application of blockchain in baggage tracking not only reduces the degree of data leakage but also enhances the privacy and security of data through utilizing the features of non-tampering of blockchain and authorized access of Consortium Blockchain.
- The multi-channel design enables the airport to rapidly process multiple types of data and business requirements in parallel, which provides coarse-grained privacy protection and promotes information sharing. It realizes the physical isolation of data and further ensures the confidentiality of transmission.
By combining RFID with the blockchain, the real-time baggage processing information is automatically stored in the blockchain, which effectively saves labor cost as well as guarantees the safety of data transmission, and improves the degree of informatization.

The integration of IPFS and blockchain realize the storage of encrypted basic baggage information in the IPFS network, while only the IPFS address Hash is stored in blockchain, which increases the scalability of the blockchain system. At the same time, the application of CP-ABE takes advantage of attribute-based encryption and provides fine-grained privacy protection.

Both software and hardware were deployed in a testbed to evaluate the performance of transaction processing time and speed for the proposed system.

The rest of this paper is organized as follows: Section II introduces related work. Section III presents the system framework, and in Section IV, we conclude design and implementation. Section V describes implementation details and result analysis. Section VI summarizes the full text.

II. RELATED WORKS

In this section, we review the related work on baggage tracking. Singh et al.[4] proposed a design of baggage tracing and handling system using smart RFID tags and IoT which is based on cloud server. However, the baggage’s real-time position is tracked and stored in a cloud, which centralized storage potentially leads to information leakage. Jerry et al.[5] proposed a system based on RFID, ZigBee and GSM to update the status of baggage at various points in the journey map. However, it does not focuses on secure information transmission and sharing. Johnson et al.[6] designed a machine vision based airport baggage tracking system using an integral image to obtain the bag location, but the huge amount of information poses a challenge to the system. Shangping Wang et al.[7] introduced a social network that combines the IPFS, Ethereum and attribute-based encryption to realize the access control to the data by setting out the access policy, but it has two problems. Firstly, the security level of Public Blockchain is excellent, but it also has slow transaction process speed and low throughput[8]. Conversely, the nodes in the Consortium blockchain do not need to keep accounts through the competitive consensus mechanism so that the consensus transaction speed is higher than Public blockchain. In addition, its authorized access mechanism can reduce the degree of data leakage and thus enhance the security of privacy data. As noted above, our system chooses HyperLedger Fabric, which is one of the most popular Consortium Blockchain platforms, as our blockchain platform. Secondly, it doesn’t focus on how information can be stored in the blockchain more securely and automatically.

III. BEI-TAB ARCHITECTURE

In this section, we illustrate the overall architecture of BEI-TAB and account for the following entities that take part in our architecture by referring to Fig.1.

• Nodes: On the one hand, the nodes in Consortium blockchain network refers to departments of airlines. There are six basic departments involved in baggage transport at one time: check-in, security check, sorting, trucking loading, air loading, and arrival. On the other hand, these nodes are also equipped with RFID readers. RFID readers obtain data from RFID tags by radio waves, which is a kind of automatic identification and data collection (AIDC) technology[9].

• Edge nodes: Edge nodes are mainly used as off-chain storage devices in our architecture. We build IPFS network among edge nodes, which stores basic luggage information data and imposes attribute-based access control policies. After uploading a file to IPFS, it returns the unique content-addressed hash while users only need this hash to access the resource[10].

• Airport: Different airports play the role of baggage information provider or visitor. Encryption policies are implemented in CP-ABE to control business access of different airport departments to ensure decentralized and secure characteristics for basic baggage information. CP-ABE is an access control technology. Private keys and ciphertexts in ABE are associated with the attributes of users or organizations. The resource providers only need to encrypt the message according to the attributes, no longer need to pay attention to the number or identity of the members in the group, which reduces the data encryption cost and protects the privacy of users[11].

• Complete baggage information: A complete piece of baggage information is divided into three parts as Fig.2 showed.

• Smart contract: The business logic of smart contract can be summarized as following three parts: 1) Combining with RFID to realize baggage tracking
information automatically stored in blockchain in real-time.
2) Providing data access and interaction interfaces for passengers and administrators respectively. Passengers can query baggage information through RFID ID to obtain the whole process of baggage tracking to reduce anxiety. The administrator can carry out accurate or batch retrieval through RFID ID and flight number so that the handling status of baggage can be grasped.
3) Generating statistics of baggage request data when passengers and management departments make real-time query requests.

The smart contract interface is shown as Table I.

Table I: Smart Contract Interface

| Interface Definition | Interface Description                           | Function Description       |
|----------------------|-----------------------------------------------|----------------------------|
| Query                | Information Query                             | Data sharing and retrieval |
| CreateZjxl           | Check-in department information               | Data access and storage    |
| CreateAxl            | Security check department information         |                            |
| CreateFx              | Sorting department information                |                            |
| CreateZhuangjxl      | Truck loading department information          |                            |
| CreateZCxl           | Airloading department information             |                            |
| CreateDj              | Arrival department information                |                            |
| QueryID              | Query the whole process information and the   | Data sharing and retrieval |
|                      | current search times through RFID ID          |                            |
| GetbID               | Query the whole process information and the   |                            |
|                      | current search times through flight number    |                            |

Our system developed a Consortium blockchain network on the Hyperledger Fabric with nodes which are check-in department node, security check department node, sorting department node, trucking loading department node, air loading department node, and arrival department node. At the same time, we deployed IPFS cluster on the edge nodes. Furthermore, the multi-channel architecture was designed to achieve physical isolation for different businesses and coarse-grained access control. The multi-channel structure refers to a channel corresponding to a business of airline company or different businesses corresponding to different channels. A channel is parallel to a Consortium blockchain. Channels are physically isolated from each other so that ledger information is only visible to the members of the channel thus providing coarse-grained privacy protection. The multi-channel design also enables the airport to rapidly process multiple types of data and business requirements in parallel. Each channel was equipped with smart contract to realize data management and sharing control. Moreover, RFID readers were also deployed on the nodes. Baggage processing information of each department is automatically recorded into the blockchain in real-time through RFID. Conversely, basic baggage information was encrypted by CP-ABE, and then written to IPFS deployed at edge nodes. Only the returned address Hash was written to the blockchain so as to enhance the scalability of the blockchain and protect the privacy of passengers. Additionally, smart contract provide interfaces for passengers and airlines, respectively. Passengers and airlines can query baggage tracking information according to RFID ID. In addition, airlines can conduct batch queries through flight number, but only those whose attributes conform to the access control policy can request basic baggage information. At the same time, smart contract calculates baggage requested data for each piece of baggage.

IV. DESIGN AND IMPLEMENTATION

As is shown in Fig.1, the hybrid architecture has specific six phrases with 14 steps that illustrated below. It mainly includes the following steps:

A. Initialization

At this stage, these entities are initialized: RFID readers, RFID tags, blockchain nodes for different departments, IPFS in edge nodes and CP-ABE encryption module. Blockchain nodes’ access control levels are detailed in Table II.

The data structure $S$ is defined within a single block. It consists of $H_i$, public data and encrypted private data. Public data includes baggage tracking information and baggage request data. Encrypted private data refers to basic baggage information encrypted by CP-ABE. Only the user whose private key completely matches the access control policy can decrypt and obtain passenger information.

B. Encrypt the basic baggage information

Step 1: The CP-ABE encryption module is initialized, and the corresponding private key is assigned according to the attributes of each part of the airport. For example, we set the property of Check-in department in airport B to
visitor Sorting `airline =861202’
`department = 05’ `identity = 2001192’
}
we set the property of Sorting department in airport A to
property Property 2 {
    admin Checkin ‘airline = 861107’
`department = 01’ `identity = 1154442’
}

Step 2: Before sharing data, Airport A needs to build an
encryption policy to achieve access control. We specify the
encryption policy \( p_i \) which allows airport A to decrypt while
airport B cannot as Rule 1. After encrypted basic baggage
information according to \( p_i \) we get \( CT_i \).

rule Rule1 {
    (admin and ( airline<861200 or
    Checkin))
    or(admin and 2 of (department > =01,
    identity > =1154442, Sorting)) }

C. \( CT_i \) is uploaded to IPFS in edge nodes

Step 3: \( CT_i \) is uploaded to the IPFS cluster to ensure not
only secure data storage, but also huge storage capacity.

Step 4: IPFS returns the address hash \( H_i \) to airport A. \( CT_i \)
can be queried in IPFS by \( H_i \).

D. \( H_i \), RFID ID, data keywords are recorded in blockchain

Step 5: After airport A got \( H_i \) from the IPFS cluster, the
RFID ID, data keywords and \( H_i \) are uploaded to the
blockchain together. Airport A can query the records in the
blockchain according to the RFID ID.

Step 6: The Consortium blockchain network returns the
inquiry result according to the requirements of airport A.

E. Baggage tracking and complete baggage information are
automatically formed and stored in blockchain.

Step 7: Airport A encodes the RFID ID, data keywords and
address hash and stores them in the user area of the RFID tag.

Step 8: Taking six departments as nodes, we build multi-
channel Consortium chain to realize physical isolation for
different companies’ businesses as well as coarse-grained
privacy protection. The program which automatically stores
data in blockchain based on Node-SerialPort and RFID is
deployed on each node. RFID readers were also deployed on
the nodes.

Step 9: When the RFID tags pass through six nodes, there
are mainly three steps:
1) RFID readers receive the data from the user area of the
RFID tag, decodes and intercepts basic baggage information.
2) Program obtains baggage tracking information automa-
tically, blends it with basic baggage information and requests
to invoke the smart contract.
3) Smart contract compares data summaries of requests and
records in the blockchain. If they are consistent, it allows data
to be stored in blockchain.

F. Data sharing and access control

Step 10: Airport B can query baggage handling status ac-
cording to RFID ID or flight number respectively. Meanwhile,
the smart contract will count the baggage tracking request
data, and the query times of each piece of baggage will be
permanently recorded in the blockchain.

Step 11: The Consortium blockchain network returns the
result to airport B, and the airport B can obtain the baggage
handling status.

Step 12: In case of lost or damaged luggage, if B demands
basic baggage information it should query its \( H_i \) of IPFS in
the blockchain according to the RFID ID, then inquires \( CT_i \)
in IPFS cluster through \( H_i \).

Step 13: The IPFS cluster finds the \( CT_i \) and returns query
results, and airport B decrypts \( CT_i \) according to its private key
\( SK_i \). Only when \( SK_i \) accord with access policy \( p \) can airport
B obtain the basic baggage information.

Step 14: Passengers can query real-time baggage tracking
information according to the RFID ID. Meanwhile, the query
times of each piece of baggage will also be recorded in the
blockchain. Administrators can conduct not only batch or
accurate retrieval, but also data interaction.

V. EXPERIMENTS AND EVALUATION

A. Experimental Setup

In this section, we implement experiments to evaluate the
performance of the proposed hybrid baggage tracking system
which was prototyped on the Hyperledger Fabric. The specific
configuration of the experimental platform and the experimen-
tal environment is: the system is deployed on 2 hosts with intel
corei7-9700@3.00GHz processor and corei7-5500@2.40GHz
processor, 4GB RAM, and we have two RFID readers.

B. Experimental Results

1) Query real-time baggage tracking information accord-
ing to the RFID ID: In the first experiment, we log into
the blockchain network as administrators. Not only can we
conduct bulk queries according to flight number but also
accurate queries by RFID ID. We can get the time of baggage
arrival in each department, flight number and IPFS address
hash corresponding to basic baggage information, as shown
in Fig.3. At the same time, this retrieval behavior will be
permanently recorded by blockchain network, and the number
of queries will plus one.

2) Test of Access Control: In the second experiment, only
when the department’s property conforms to the access control
policy can it decrypt basic baggage information downloaded
from IPFS. For instance, the access policy we developed in
attribute-based access control allows all departments in airport
A to decrypt basic baggage information while airport B cannot,
as shown in Fig.4.

3) System Performance: We conducted four rounds of
tests to measure the average time for RFID data to store
in blockchain. To evaluate the scalability of our system,
we also carry out extensive system performance evaluations
by increasing the number of baggage and departments. The
average time for RFID data to store in the blockchain from 4 rounds of tests remains at around 0.58 s when the number of baggage increased from 6 to 1000 as shown in Fig.5. The results of the experiments show that when the number of baggage and departments increased, transaction time and response time did not change significantly, which demonstrates that the performance of the proposed system is scalable. The prototype system can realize baggage processing information stored in the blockchain in real-time and automatically as well as produce response in a few hundred milliseconds, which makes it suitable in practical baggage tracking systems.

VI. CONCLUSION

In this paper, we have proposed a system named BEITAB that utilized RFID combined with Consortium blockchain to realize the real-time tracking information automatically stored in the blockchain, which not only avoids data leakage but also improves the industrialization level of the airport. In addition, we took advantage of multi-channel architecture realized physical isolation of different businesses and coarse-grained privacy protection. At the same time, we utilized CP-ABE and IPFS to store basic baggage information in edge nodes so as to improve the scalability of blockchain and provide fine-grained privacy protection. To this end, we have deployed a testbed with both software and hardware to evaluate the performance of transaction processing time and speed. The experiments showed that our system is scalable, which makes it suitable to be incorporated in secured and real-time baggage tracking.

REFERENCES

[1] T. Ahmed, T. Calders and T. B. Pedersen, “Mining risk factors in RFID baggage tracking data,” 2015 16th IEEE International Conference on Mobile Data Management, Pittsburgh, PA, USA, 2015, pp. 235-242, doi: 10.1109/MDM.2015.31.
[2] R. Yang, F. R. Yu, P. Si, Z. Yang and Y. Zhang, “Integrated blockchain and edge computing systems: a survey, some research issues and challenges,” IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1508-1532, Secondquarter 2019, doi: 10.1109/COMST.2019.2894727.
[3] Huang, H., Lin, J., Zheng, B., Zheng, Z., Bian, J. (2020). “When blockchain meets distributed file systems: an overview, challenges and open issues,” IEEE Access, 8, 50574-50586. doi:10.1109/access.2020.2979881.
[4] A. Singh, S. Meshram, T. Gujar and P. R. Wankhede, “Baggage tracing and handling system using RFID and IoT for airports,” 2016 International Conference on Computing, Analytics and Security Trends (CAST), Pune, 2016, pp. 466-470, doi: 10.1109/CAST.2016.7915014.
[5] M. S. Jerry, M. M. Vijay and T. K. Tulshiram, “Carousel security management and cargo deck tracking of passenger baggage using wireless technology,” 2016 IEEE Bombay Section Symposium (IBSS), Baramati, 2016, pp. 1-6, doi: 10.1109/IBSS.2016.7940195.
[6] M. Johnson and A. Gilman, “Real-time baggage tracking using a modified background subtraction algorithm,” 2012 19th International Conference on Mechatronics and Machine Vision in Practice (M2VIP), Auckland, New Zealand, 2012, pp. 200-204.
[7] S. Wang, Y. Zhang and Y. Zhang, “A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems,” IEEE Access, vol. 6, pp. 38437-38450, 2018, doi: 10.1109/ACCESS.2018.2851611.
[8] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the internet of things,” IEEE Access, vol. 4, pp. 2292-2303, 2016, doi: 10.1109/ACCESS.2016.2566339.
[9] Juels, A. (2006). “RFID security and privacy: a research survey,” IEEE Journal on Selected Areas in Communications,24(2), 381-394. doi:10.1109/jsac.2005.861395.
[10] R. Norvill, B. B. Fitz Pontiveros, R. State and A. Cullen, “IPFS for reduction of chain size in Ethereum,” 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 2018, pp. 1121-1128, doi: 10.1109/Cybermatics2018.2018.00204.
[11] J. Bethencourt, A. Sahai and B. Waters, “Ciphertext-policy attribute-based encryption,” 2007 IEEE Symposium on Security and Privacy (SP ’07), Berkeley, CA, USA, 2007, pp. 321-334, doi: 10.1109/SP.2007.11.