Aviation Terminal Data Security Architecture Based on Blockchain

Zhiwei Chen\textsuperscript{1,3}, Aidong Xu\textsuperscript{2}, Hong Wen\textsuperscript{1,3}, Yunan Zhang\textsuperscript{2} and Xinchen Xu\textsuperscript{1,3}

\textsuperscript{1} School of Aeronautics and Astronautics, University of Electronic Science and Technology of China, Chengdu 611731, China
\textsuperscript{2} EPRI, China Southern Power Grid Co. Ltd., Guangzhou, China.
\textsuperscript{3} Aircraft Swarm Intelligent Sensing and Cooperative Control Key Laboratory of Sichuan Province, UESTC, Chengdu 611731, China
Email: sunlike@uestc.edu.cn

Abstract. With the advent of the 5G era, the number of UAV (Unmanned Aerial Vehicle) has grown dramatically. Accordingly, UAV need more computing and storage capabilities to complete a variety of tasks (including some collaborative tasks). To meet the requirements of UAV terminals, edge computing nodes and storage devices need to be deployed. But the problem of trust between edge computing nodes will lead to a series of data security problems. The blockchain features, which contain detrust, immutable, decentralized, can solve this problem properly. Therefore, this paper establishes an aviation terminal data security architecture based on the blockchain. Edge computing nodes and storage devices provide computing and storage resources for UAVs. As the core operating mechanism of the architecture, blockchain technology guarantees that the system has Byzantine fault tolerance performance through its consensus algorithm. The blockchain data structure under this architecture also guarantees that the data access records of all nodes will be written on the ledger and the ledger is stored by all miner nodes.

1. Introduction

As aviation terminals are no longer limited to large passenger aircraft such as airplanes and helicopters, the number of UAV (Unmanned Aerial Vehicle) will continue to increase in the future, which will generate a large amount of data and a network between the UAVs. With the advent of the 5G era, the scope of UAV applications has also greatly expanded. UAV have been mainly used in the military field since the first successful test flight in 1917. Since 2006, a large number of private enterprises have entered the UAV industry, and the UAV industry has begun to enter a period of rapid growth. The use of UAV has begun to shift from military to civilian. With the emergence of a new generation of 5G wireless communication technology, a highly reliable, low-latency, wide-coverage data link system is provided for UAV which means more UAV applications for the masses will be generated and the process of UAV networking will be accelerated. Trusted access of UAV to the network and trusted sharing of massive data of UAV become the key problem to be solved.

There are many methods to ensure the data security (e.g. Attribute-based encryption, proxy re-encryption, secure data search). But most methods focus on the confidentiality, integrity and availability of the data layer instead of its architecture [1]. Some physical layer security enhancements are also applied in the related field [5]. With the continuous development of blockchain technology, many related fields use blockchain as its emerging technology [2] (e.g. Internet finance, digital government, logistics Fields, Internet of things). Blockchain organizes data in blocks and all the transaction records of the entire network are stored in the unique blockchain. The immutable, traceable,
and de-trusted features of the blockchain technology which are based P2P network can ensure the security of data.

This paper will propose a blockchain-based aviation terminal data security architecture to provide UAV data storage services and computing services while ensuring data security in untrusted UAV networks.

2. Cloud Computing & Edge Computing in Aviation Terminal

2.1. Cloud Computing in Aviation Terminal

Cloud computing has taken the world by storm. In this category of utility computing, a collection of computing resources (e.g. network, servers, storage) are pooled to serve multiple consumers, using a multi-tenant model. These resources are available over a network, and accessed through standard mechanisms.

Due to the development of UAV network and the 5G wireless communication technology, real-name authentication of the UAV can be achieved and connected to the UAV cloud system. The UAV cloud system can provide some service for the UAV (e.g. storage, network, servers). However, this centralization of resources implies a large average separation between end user devices and their clouds, which will cause some fatal weaknesses.

- Increase the average network latency.
- Cloud services are not able to directly access local contextual information.

2.2. Edge Computing in Aviation Terminal

Due to the shortcomings of cloud computing architecture, an edge computing architecture has emerged in recent years, which can expand cloud servers to the edge side which is close to end users. This architecture establishes micro data centres in the different geographic locations. When generating and requesting data, end users generally obtain it from the local edge micro data centre, and perform real-time processing and controlling on the edge data centre. [5]

![Edge computing architecture](image)

**Figure 1.** Edge computing architecture

And the edge data centre will interact with the cloud when the huge data that needs to be stored for a long time or some complex computing tasks that need to be processed. After that, the cloud side will use its computing resources or storage resources to cooperate with the edge data centre and the data will be securely processed and stored by the cloud server. Both the edge side and the cloud side
establish strategies for secure data exchange and data access. at the same time, the cloud can manage and coordinate multiple edge micro data centres. This architecture has the following advantages:

- It can greatly reduce the network delay caused by geographical factors in the cloud computing.
- Cloud services can obtain the user's mobile behaviours information, predict geographic location information, and local network conditions.
- It can greatly reduce the load pressure on the cloud centre server, and suppress a single point of failure to a certain extent.
- Data centre is close to the terminal, security and privacy protection is easier to implement.
- Improve the flexibility and scalability of the entire system.

But this architecture also has some security threats, as shown in the table below [6]:

| Security Threats | Core Infrastructure | Edge Servers | Edge Network | Mobile Edge Devices |
|------------------|---------------------|--------------|--------------|---------------------|
| Privacy leakage  | Privacy leakage     | Denial of service | Injection of information |
| Data tampering   | Denial of service   | Privilege escalation | Man-in-the-middle |
| Denial of service| Service manipulation| Service manipulation | Rogue gateway |
| Service manipulation | Rogue data centre | Physical damage | |

There are many security mechanisms to ensure data security in edge computing (e.g. Trust management, data encryption, access control system, Identity and authentication). But the distributed and detrust nature of the blockchain provides new ideas for designing frameworks and paradigms for edge computing.

3. Blockchain Based Data Security Architecture in Aviation Terminal

3.1. Blockchain Technology Architecture

| Application layer | Programmable currency | Programmable finance |
|-------------------|-----------------------|----------------------|
| Contract layer    | Smart contract        | Script code          |
| Consensus layer   | Consensus algorithm   | Incentives           |
| Network layer     | P2P network           | Communication mechanism |
|                   | Authentication mechanism |
| Data layer        | Data block            | Chain structure      |
|                   | Merkle tree           | Asymmetric encryption |
|                   | Hash function         |                      |

**Figure 2.** Blockchain architecture

As shown in the figure 2, the blockchain can be divided into five layers, and this paper will introduce the role of each layer by explaining blockchain operation mechanism:

- First, you generate some transaction, and you broadcast the transaction to the blockchain network.
• Then, a lot of miners in the blockchain can collect transactions through P2P networks and verify the legality of the transaction or execute the smart contract in it. After that, miner will package these transactions into block with previous block hash.
• All miner nodes in the blockchain will reach a consensus through some consensus algorithm. And after that, miner nodes that collect these legal transactions will be rewarded.
• The newly generated block will be broadcast to the blockchain network, and all miner nodes will synchronize the block information.
• All the miners will store the ledger that contain all the blocks.

Figure 3. Blockchain data structure

The blockchain data structure is shown in the figure 3, due to the one-way nature of the hash function and the characteristics of the chain structure, every malicious node that wants to change the block information must modify all subsequent blocks. This data layer guarantees that the data on the blockchain cannot be tampered.

On the other hand, the consensus mechanism also provides a Byzantine fault-tolerant opportunity for the blockchain network. When malicious nodes exist in the blockchain network, as long as the proportion of malicious nodes is lower than a certain value (this certain value depends on the design of the consensus algorithm), the group's decision will not be controlled by malicious nodes.

3.2. The Combination of Blockchain Technology and Edge Computing for the UAV Network
The development of 5G mobile communication technology has led to the rapid development of the process of UAV network. Data storage of UAV and data access between UAVs which are in the same UAV cluster have become an important issue. UAV terminals are lightweight terminals. Its main computing resources and storage resources are very limited because of the flight mission. If the UAV task needs to store a large amount of data for a long time or perform a large computing task, the UAV itself cannot complete, which will greatly limit the application scenarios of the UAV.

This paper proposes a blockchain-based aviation terminal data security architecture to break through the restrictions of UAV computing resources and storage resources. As shown in the figure 4 below:
According to the above figure, it can be seen that the system architecture is mainly composed of UAV, P2P peer-to-peer networks, user equipment, edge computing nodes, data storage devices, and server clusters. The function of each part will be explained as follows:

- **UAV**: UAV need to collect, store, and process data information, and return these data information to user equipment. However, due to the needs of flight, the computing and storage resources are occupied, the UAV is lightweight node and interact with edge computing nodes when the UAV need to access some data from other UAVs or upload some data that users need.

- **P2P network**: The P2P network is connected to each node in the system based on the TCP protocol, and transaction can be broadcasted by the node in this blockchain.

- **Edge computing nodes**: Due to the limited computing capabilities of the UAV, these nodes are added to the blockchain network. These nodes have powerful computing capabilities, which can complete the task of data encryption, and the consensus process in the blockchain network.

- **Data storage devices**: Since the limitation of the UAV storage resources and computing resources, the UAV cannot store and encrypt the data that users need. Therefore, the data will be encrypted by the edge computing nodes. After that, the ciphertext will be stored in the data storage devices instead of blockchain to improve the scalability of the blockchain and the efficiency of edge computing nodes.

- **Server cluster**: The transaction will be recorded on the blockchain only when the transaction is legal and all the miners reach a consensus. And the server clusters are also the miner nodes in the blockchain, which will protect the blockchain from being controlled by the malicious nodes.

Under this architecture, when the UAV needs to store data. The following steps will be required:

Step 1: The UAV will interact with edge computing nodes to send a request for data storage and create access policies.

Step 2: The edge computing node broadcasts the transaction, and the nodes on the blockchain network will verify the identity of the UAV and reach a consensus.

Step 3: The UAV stores the data in the edge data storage device, and records the data access strategy on the blockchain.

When a UAV needs to access data in an edge data storage device, it will need to perform the following steps:

Step 1: The UAV interacts with the edge computing node and sends a data access request.
Step 2: The edge computing node will broadcast the transaction, and the nodes on the blockchain network will verify the identity of this UAV and whether the request satisfies the data access policies and reach a consensus.

Step 3: The edge computing node will return the data to the UAV and this access behaviour will be written on the blockchain permanently, which will be stored by the miner nodes on the blockchain.

This architecture eliminates the limitations of UAV computing and storage resources by deploying edge computing nodes and data storage devices. On the other hand, there is a lack of trust between edge computing nodes. In order to ensure the data security in this untrusted UAV network, a blockchain framework was introduced. The data will be encrypted by the edge computing nodes and stored in the data storage device. The access policies are deployed by the smart contracts on the blockchain. When a node on the blockchain needs to access the data resources of other nodes, it needs to call the smart contract on the blockchain and the miners will execute the smart contract and verify its access permissions. When the miners in the blockchain reach a consensus, which means the access request satisfies the access policies, its behaviour of accessing other database resources will be recorded permanently by the blockchain.

4. Conclusion
This paper proposed a blockchain based aviation terminal data security architecture, which not only has the advantages of edge computing (e.g. it can quickly obtain the computing and storage resources of edge nodes) but also ensures the security of UAV data in a untrusted network which contains a lot of untrusted edge computing nodes through the cryptographic principles of the blockchain architecture (e.g. key distribution mechanism, zero-knowledge proof algorithm, hash function, Merkle tree structure) and consensus mechanism (e.g. POW, POS, PBFT)

5. Acknowledgement
This research is supported by the National Key R&D Program of China (2018YFB0904900, 2018YFB0904905).

6. References
[1] Qing Yang, Yixin Jiang, Aidong Xu, Hong Wen, Feng Wang, LiuFei Chen, Kai Ouyang, Xinping Zhu, “A Model Divides the Mobile Security Level Based on SVM,” in Proceedings of IEEE CNS 2017, LasVegas, USA, 7-9 Oct., 2017.
[2] LiuFei Chen, Yushan Li, Hong Wen, Wenxin Lei, Wenjing Hou, Jie Chen, Block Chain Based Secure Scheme For Mobile Communication, CNS2018
[3] Lin Hu, Hong Wen, Bin Wu, Fei Pan, Run-Fa Liao, Huanhuan Song, Jie Tang, Xiumin Wang, Cooperative Jamming for Physical Layer Security Enhancement in Internet of Things, IEEE Internet of Things Journal, Vol. 5, Issue 1, pp. 219-228, 2018.
[4] H Wen, PH Ho, B Wu, Achieving secure communications over wiretap channels via security codes from resilient functions, IEEE Wireless Communications Letters 3 (3), 273-276
[5] F Xie, H Wen, Y Li, S Chen, L Hu, Y Chen, H Song, Optimized coherent integration-based radio frequency fingerprinting in Internet of Things,IEEE Internet of Things Journal 5 (5), 3967-3977
[6] Roman R, Lopez J, Mambo M. Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. Future Generation Computer Systems, 2018, 78: 680-698
[7] Zhang J, Chen B, Zhao Y, et al. Data security and privacy-preserving in edge computing paradigm: Survey and open issues. IEEE Access, 2018, 6: 18209-18237.