Internet of Drone: Identity Management using Hyperledger Fabric Platforms

Igugu Tshisekedi Etienne*, Sung-Won Kang**, Kyung-hyune Rhee***
*Dept. of Information Security, Pukyong National University
**Dept of Artificial Intelligence Convergence, Pukyong National University
***Division of Computer Engineering, Pukyong National University

Abstract

The uses of drones are increasing despite the fact that many of us are still skeptical. In the near future, the data that will be created and used by them will be very voluminous, hence the need to find an architecture that allows good identity management and access control in a decentralized way while guaranteeing security and privacy. In this article, we propose an architecture using hyperledger fabric blockchain platform which will manage the identity in a secure way starting with the registration of the drones on the network then an access control thanks to Public Key Infrastructure (PKI) and membership service provider (MSP) to enable decision-making within the system.

1. Introduction

Today, companies dream of leveraging drones with an advanced vision of their uses because they have great mobility and provide multiple solutions in several areas such as civil, industrial, and military applications. This technology also presents new market opportunities for various assistance such as telecommunications relay stations, delivery of packages, surveillance to protect a sensitive site, taking of images, monitoring or spreading of pesticides in a specific area in agriculture, etc. Accordingly, all collected data will be sent to a control and storage center via a network.

This article presents a solution to improve storage security and data sharing within the Internet of drones (IoD). A proposed solution will ensure confidentiality, authentication and security of communication between drones and the control center. After analyzing the issues presented by other researchers related to data security between drones, a system using blockchain is needed to encrypt and decentralize data within the network, this system can control drone identity without a central authority, it enables drone to share their identity according to other drone and can protect user's consent [1].

The rest of the paper is organized as follows: Section 2 will present an overview of drone and drone communication, and the technologies used for internet of drones security enabled data storage and sharing; Section 3 gives the blockchain platform for architecture of the network, the motivation, and the function of the system; Section 4 provides concluding remarks.

2. Overview

This section will introduce the concepts of the Internet of Drones and the technology we will be using. First, by presenting the drone, then its network architecture, and finally the blockchain that we will propose in this article as a better solution for the security and privacy.

2.1. Drone

Drones are unmanned aerial vehicles capable of traveling autonomously over several kilometers or by being remotely controlled by an operator. Their ability to be remotely controlled has enabled them to be used in several situations and applications where humans are limited either by inaccessibility or by danger [2]. However, drones vary according to the technologies used, their applications, types, and their architectures, which allow them to carry out several different operations depending on their field of activity.

2.2. Drone Network Architecture

The architecture of the drone network is divided into two parts; (1) a control center located on the ground which is a management system for this network, and (2) the different drones in the network which can perform calculations and storage. For this network architecture, drones represent the nodes that form a mesh network; the whole drone acts as a single wireless network that facilitates the use of blockchain technology [3].

This includes the flexibility of network coverage by allowing additional nodes to be added without disrupting the network; making all nodes interconnected. While in automatic network repair, when a node ceases to function for any reason, its signal will simply be redirected to another node and then stabilizes a direct. In this way, data can take multiple path to reach its destination. As it will always be necessary to take the fastest route from point A to point B, this architecture makes it possible to cover a much larger area, and the cost of the equipment is lower.

The control center is the network management system that facilitates communication and data exchange with drones during their mission and assigns the missions to the drone and defines the initial flight plan.

Once on a mission, the drone will automatically update its geographic position and location on the network and will communicate it within the network to enable other drones to detect and locate it geographically. An identification list point out the identifier of the drone, its role and the on-board equipment managed will be distributed in the network; creating strategic data necessary for the communication of drones in the network [3].

2.3. Blockchain

Blockchain is a technology used to encrypt the database ledger. This technology contains several blocks chained in a linear and chronological way, each block uses a unique identification and has a hash of the previous block which is recorded in its header [4]. Data is permanently stored on the network in blocks to allow decentralization and dissemination. The blockchain uses the hash function to connect the blocks in a tamper-proof way, it uses the digital signature to verify the identity of the user to ensure the integrity and non-repudiation and generate public and private keys, the private key is used to encrypt messages or data while a public key is used for decryption and verification [5].

3. Internet of Drone using Hyperledger Fabric Platforms

In this section, we focus on node registration and data storage preserving privacy. As well as the right of access for identity/data privacy protection, along with a flexible sharing approach to store data based on blockchain using hyperledger fabric platform.

3.1. Motivations

Indeed, drones are faced with many problems due to their massive and unsafe use in an open environment. A drone or malicious user can collect data such as identity information, shared data, and operating information from a target drone without being detected. The attacker can plan to perform his attack on a target using all the information he already has. It can divert a drone from its original route, it can cause a collision with other drones or with aircraft, and all of these generate a challenge for information security and confidentiality of data transmission and can produce damage considerable.

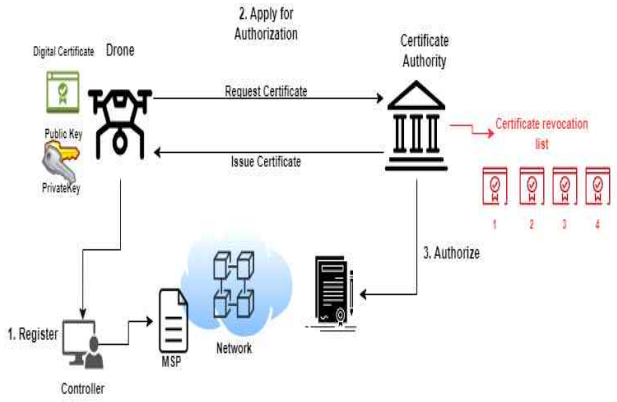
A drone data-sharing model based on blockchain is needed because blockchain is used to create an environment with a trust mechanism solely based on privacy protection. On the other hand, the information can be seen by other users on the blockchain, hence the need to use a blockchain platform that will make the data

visible only to the members of the same channel[6].

3.2. Our Work

According to the official documentation [7], hyperledger fabric is a blockchain platform used to create a private and permissioned host; which offers a high-performance, secure, scalable and confidential network.

In IoD application hyperledger fabric offers Identity Management Figure 1. All drones have to register to the network and receive an digital identity. Hyperledger fabric manages the identities and authentication of all drones in the network and can create a drone group, which will have a separate disclosed ledger that will avoid disclosing a transaction to other drones in the network which are not of the group.

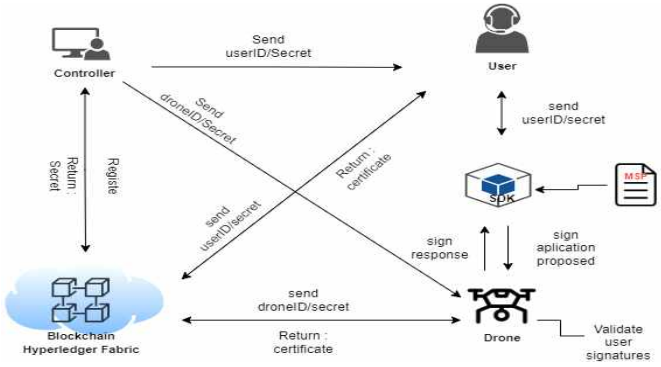


(Figure 1) Hyperledger fabric identity management

A verified identity is one that comes from the list of PKI (Public Key Infrastructure); a MSP (Membership Service Provider) is the trusted authority of the platform, an MSP is determined that its drone is valid or not by using a PKI list. Identities have attributes that allow Hyperledger fabric to assign permissions. Any node with a certificate is called Principal; a principal can use its ID or the ID of the group it belongs to. This authorization operation feature provides access control as PKI and MSP work together; PKI provides an Identity list and MSP makes the decisions. As an example, in PKI containing drone identifiers those registered by a network controller A are authorized to perform a task by running a chainCodes (smart contract) or to integrate member group and the drones that have not been registered by this controller A can not get access to it and because their certificate are in a Certificate revocation list.

3.3 Authentification and Validation

Membership Service Provider (MSP) is a Hyperledger Fabric component that determines a member of a trusted domain; an MSP supports all the cryptographic mechanisms and protocols behind certificate issuance, certificate validation, and user authentication [7].



(Figure 2) Hyperledger fabric identity management

Figure 2 shows a Hyperledger structure integrated with IoD by customizing the interaction within the system. A Hyperledger Fabric SDK supports applications developed in multiple programming languages such as Java, Go, and Python; an SDK can be created or an existing one will be used as middleware. This system is responsibility-based, which means that every node in the network must authenticate. Identities are assigned by the MSP and the CA uses a PKI to approve and validate a node.

The controller or administrator registers the identity of the drone and the user; it fixes the organization and helps the new node to integrate into the network, with each node registration the system returns a secret key linked to the identity; the admin sends it to the drone and the user his identifier and his secret key. For authentication, each node sends its ID and the secret key to the Certification Authority (CA) to obtain a certificate

and the user signs his action to receive the validation of the drone in the application; the MSP of SDK contains a list of certified users, list of certified drones, list of revoked certificates and application to run in a channel.

4. Conclusion

With the current technological advancements regarding drones, they are becoming more accessible to the general public, which makes them capable of collecting, storing, analyzing and transmitting personal or professional data. The identification of the latter remains a big problem because from their conception it has been neglected, this is the main reason why their use is prohibited in certain areas or outright rejected by other authorities because of the lack of the infrastructure dedicated to identification.

Thus, in this article, we propose a system capable of managing the identification and authentication of drones using a blockchain platform which brings many advantages, advanced confidentiality which makes it possible to give access only to the desired drones between the authorized participants of the network, other advantages are linked to the fact that we can create a private channel, we can use a Java programming language for the creation of chainCode (smart contract), there is no currency to perform a transaction and information can be queried from the registry as SQL queries.

Acknowledgement

This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITP(Institute for Information & Communications Technology Planning & Evaluation) (IITP-2022-2020-0-01797) and Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(2021R1I1A3046590)

References

1. Saraf, C., &Sabadra, S, “Blockchain platforms: A compendium,” 2018 IEEE International Conference on Innovative Research and Development (ICIRD) pp. 1-6, 2018
2. M. Hassanalian and A. Abdelkefi, “Classifications, applications, and design challenges of drones: A review,” Aerospace Sciences, 91:99 - 131, 2017
3. Mohannad Alharthi, Abd-Elhamid M Taha, and Hossam S Hassanein, “An architecture for software defined drone networks,” 2019 IEEE International Conference on Communications (ICC), pp. 1 - 5. 2019.
4. Y. Wu, H. N. Dai, H. Wang, and K. K. R. Choo, "Blockchain-based privacy preservation for 5g-enabled drone communications," IEEE Network, 35(1):50 - 56, 2021.
5. Bhabendu Kumar Mohanta, Debasish Jena, Soumyashree S. Panda, and Srichandan Sobhanayak. "Blockchain technology: A survey on applications and security privacy llenges," Internet of Things, 8:100-107, 2019.
6. F. Benhamouda, S. Halevi and T. Halevi, "Supporting private data on Hyperledger Fabric with secure multiparty computation," IBM Journal of Research and Development, 63(2/3)3:1-3:8, 2019, doi: 10.1147/JRD.2019.2913621.
7. “Hyperledger Fabric Project,” https://hyperledger-fabric.readthedocs.io/en/release-2.2/ [Accessed: 22-April-2022].