Cloud Controlled Unmanned Aircraft System Cybersecurity

Caleb Leeb, Anthony Johnson, Shubham Nipanikar, & Russell Rozensky

Embry-Riddle Aeronautical University

Abstract

Integrating a small, unmanned aircraft system (sUAS) with cloud capabilities for military or enterprise use has not usually been widely feasible due to cybersecurity concerns. With recent advancements in blockchain networks the possibility of large cloud connected UAS networks has emerged. Our team investigates how to integrate data collected from a sUAS with a cloud-based service for data collection, storage, and processing implemented to ensure data privacy and data integrity. Our proposed network architecture utilizes a general purpose blockchain network in order to maintain decentralized network security. Research objectives include running security tests against a blockchain network & host/client networks, then comparing their performance and abilities to support the cloud based UAS. Specifically, we are using an open-source project called AirSim to support a virtual UAS that is connected to the UAS flight controller, the Pixhawk, to test a hardware-in the loop solution. This test is a preliminary proof of concept, and after it proves successful, we are moving to a test involving a physical UAS. Data is transmitted from the UAS to a client server in Amazon Web Services (AWS) where it is placed into a blockchain network and sent to the host server for processing. Overall, we believe a private blockchain network supporting cloud-enabled communication can be an effective method of bolstering secure and responsive UAS communications.

Full Architecture Overview

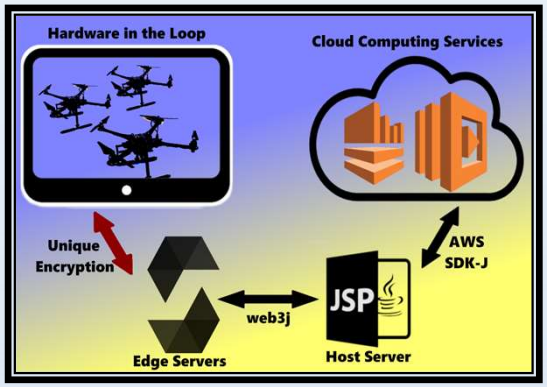

Figure 1. This diagram depicts the basic relationship for how data would be transmitted and dispersed among nodes.

Research Questions

Confidentiality:

1. To what extent can blockchain secure the offloading of UAS-gathered data as compared to other methods?

Integrity:

1. How can blockchain maintain integrity by either deterrence or self-correction?
2. How difficult is it to take control of a UAS via spoofing through a cloud-based system using blockchain as compared to legacy encryption standards?

Availability:

1. How can a UAS System securely recover in real time when one GCS loses contact?
2. How can a private blockchain network absorb a Denial of Service (DoS) attack in real time to prevent loss of connection to a UAV?

Data Transfer Overview

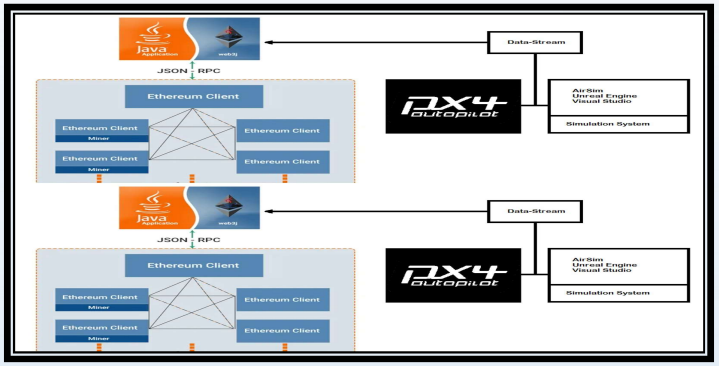

Figure 2. This diagram depicts how data will pass from the cloud server and onto the blockchain in Ethereum

Recommendations for Future Research

- Direct one to one connection of each client account to a separate kinesis stream via Kinesis Firehose.
- Software as a Service (SaaS) with distributed file systems via blockchain, using this in private sector securely encrypted shared file.
- Discussion on possibility of middleware into java operations, minimizing computational overhead via an interface for pure java computation rather than continuous changes to the ledger. Discuss possible concerns of security in communicating to this unencrypted server.
- Integrate an industry standard Ground Control Station (GCS) like Piccolo Command Center (PCC) & PCC CoPilot with proposed solution to demonstrate practicality with larger systems.

Potential Applications

- Small Unmanned System (sUAS of DoD Group One Size) that is man-portable (MANPAD) and rapidly deployable for Special Operations Forces (SOF) teams for the purpose of unit-specific Intelligence, Surveillance, and Reconnaissance (ISR) collection, easily deployable in firefights, and potentially capable of lasing targets. [11]
- An sUAS that is a MANPAD platform usable by standard combat arms Soldiers/Marines that could be used for general ISR collection, target tracking and locating (for artillery and armor units), and for employing general situational awareness. This could bode extremely useful for Soldiers/Marines deployed in extremely stressful urban environments. [10]
- A larger UAS, not of MANPAD size (DoD Group Two Size), but comparable to the Aerosonde platform that is supported by our system to bring advanced loitering ISR capabilities/missions with a relatively small surveillance team.

Figure 3. A Soldier with the (sUAS) Black Hornet Airborne Personal Reconnaissance System (PRS) by FLIR [10].

References

[4] M. Alharthi, A. M. Taha and H. S. Hassanein, "An Architecture for Software Defined Drone Networks," *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, Shanghai, China, 2019, pp. 1-5, doi: 10.1109/ICC.2019.8761968.

[5] Yapp, Justin, "UAV as a Service: Providing On-Demand Access and On-The-Fly Retasking of Multi-Tenant UAVs Using Cloud Services", *Dissertations and Theses*. 2016. 259.

[6] Rodrigues, M., Pigatto, D. and Branco, K., 2018. Cloud–SPHERE: A Security Approach for Connected Unmanned Aerial Vehicles. In: *International Conference on Unmanned Aircraft Systems (ICUAS)*. Dallas, Texas: IEEE.

[8] Blockchain integrated Cloud of Things (talking about this as an architecture and acknowledging its existence) Integration of Blockchain and Cloud of Things: Architecture, Applications and Challenges https://ieeexplore-ieee-org.ezproxy.libproxy.db.erau.edu/document/9179702/

[10] Deptula, David A., and James R. Marrs. "Global Distributed ISR Operations- The Changing Face of Warfare." *DOD Report*, no. OMB No. 0704-0188, 2009.

[11] Best, Richard A. "Intelligence, Surveillance, and Reconnaissance (ISR) Programs: Issues for Congress." *Congressional Research Service*, no. OMB No. 0704-0188, 4 Aug. 2004.

[12] M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung and M. Song, "Performance Optimization for Blockchain-Enabled Industrial Internet of Things (IIoT) Systems: A Deep Reinforcement Learning Approach," in *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3559-3570, June 2019

[13] Y. Liu, F. R. Yu, X. Li, H. Ji and V. C. M. Leung, "Decentralized Resource Allocation for Video Transcoding and Delivery in Blockchain-Based System With Mobile Edge Computing," in *IEEE Transactions on Vehicular Technology*, vol. 68, no. 11, pp. 11169-11185, Nov. 2019

[15] Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." 31 Oct. 2008.

[17] Salhaoui, M., Guerrero-González, A., Arioua, M., Ortiz, F. J., El Oualkadi, A., & Torregrosa, C. L.. Smart Industrial IoT Monitoring and Control System Based on UAV and Cloud Computing Applied to a Concrete Plant. Sensors (Basel, Switzerland), 19(15), 2019: 3316.