drones

Article

LightMAN: A Lightweight Microchained Fabric for Assurance- and Resilience-Oriented Urban Air Mobility Networks

Ronghua Xu [1], Sixiao Wei [2], Yu Chen [1,*], Genshe Chen [2] and Khanh Pham [3]

1 Department of Electrical and Computer Engineering, Binghamton University, Binghamton, NY 13902, USA
2 Intelligent Fusion Tech, Inc., Germantown, MD 20876, USA
3 The U.S. Air Force Research Lab, Space Vehicles Directorate, Albuquerque, NM 87110, USA
* Correspondence: ychen@binghamton.edu

Abstract: Rapid advancements in the fifth generation (5G) communication technology and mobile edge computing (MEC) paradigm have led to the proliferation of unmanned aerial vehicles (UAV) in urban air mobility (UAM) networks, which provide intelligent services for diversified smart city scenarios. Meanwhile, the widely deployed Internet of drones (IoD) in smart cities has also brought up new concerns regarding performance, security, and privacy. The centralized framework adopted by conventional UAM networks is not adequate to handle high mobility and dynamicity. Moreover, it is necessary to ensure device authentication, data integrity, and privacy preservation in UAM networks. Thanks to its characteristics of decentralization, traceability, and unalterability, blockchain is recognized as a promising technology to enhance security and privacy for UAM networks. In this paper, we introduce LightMAN, a lightweight microchained fabric for data assurance and resilience-oriented UAM networks. LightMAN is tailored for small-scale permissioned UAV networks, in which a microchain acts as a lightweight distributed ledger for security guarantees. Thus, participants are enabled to authenticate drones and verify the genuineness of data that are sent to/from drones without relying on a third-party agency. In addition, a hybrid on-chain and off-chain storage strategy is adopted that not only improves performance (e.g., latency and throughput) but also ensures privacy preservation for sensitive information in UAM networks. A proof-of-concept prototype is implemented and tested on a micro-air–vehicle link (MAVLink) simulator. The experimental evaluation validates the feasibility and effectiveness of the proposed LightMAN solution.

Keywords: unmanned aerial vehicle (UAV); lightweight blockchain; drone security; assurance; authentication; resilience

check for updates

Citation: Xu, R.; Wei, S.; Chen, Y.; Chen, G.; Pham, K. LightMAN: A Lightweight Microchained Fabric for Assurance- and Resilience-Oriented Urban Air Mobility Networks. *Drones* **2022**, *6*, 421. https://doi.org/10.3390/drones6120421

Academic Editors: Ivana Semanjski, Antonio Pratelli, Massimiliano Pieraccini, Silvio Semanjski, Massimiliano Petri and Sidharta Gautama

Received: 31 October 2022
Accepted: 13 December 2022
Published: 16 December 2022

1. Introduction

Thanks to rapid advancements in artificial intelligence (AI), big data, information fusion, and Internet of Things (IoT) technologies, it has become realistic for the concept of smart cities to provide seamless, intelligent, and safe services for communities [1,2]. As a class of robotic vehicles in the IoT, unmanned aerial vehicles (UAV), commonly known as drones, are widely adopted in smart city scenarios for sensing data, carrying payloads, and performing specific missions guided either by remote control centers or in autonomous ways [3]. Thanks to fifth-generation (5G) communication networks and mobile edge computing (MEC) technology, UAVs demonstrate higher mobility than other robotic vehicles, and they can provide on-the-fly communication capabilities in a remote area where terrestrial infrastructure is under-developed or disaster-struck areas where physical or technology has infrastructure been destroyed [4]. Moreover, drones equipped with different types of sensors, such as environmental sensors or cameras, can form UAV networks to guarantee better quality-of-service (QoS) or quality-of-experience (QoE) for users who demand a large number of network-based intelligent services in smart cities, such as video surveillance [5], disaster management, smart transportation, medical suppliers, and public safety [6,7].

With an ever-increasing presence of UAVs in urban air mobility (UAM) networks, the highly connected internet of drones (IoD) also raises new concerns on performance, security, and privacy. On an architectural level, conventional UAV-enabled applications rely on a centralized framework, which is prone to a single point of failure (SPF). As centralized servers coordinate flying drones and perform decision-making tasks, the entire UAV system may be paralyzed if control centers experience malfunctions or are under attacks such as denial of service (DoS) attacks. In addition, complete centralized frameworks that swarm a large number of distributed drones are prone to performance bottlenecks (PBN). As a result, increasing end-to-end network latency degrades QoS or QoE in real-time applications. Moreover, the dynamicity of UAV networks including resource-constrained drones also meets security and privacy challenges within a distributed network environment. Security threats that can severely affect UAV networks can be categorized as firmware attacks (e.g., false code injection, firmware modification, malware infection, etc.) and network attacks (e.g., spoofing, jamming, command injection, network isolation, etc.) [8]. Owing to encrypted data transmission between drones and unauthorized access to data stored on servers, privacy breaches lead to revealing sensitive information such as location, flying path, or other identity-related data.

Thanks to multiple attractive features, such as decentralization, immutability, transparency, and traceability, blockchain has demonstrated great potential to revolutionize centralized UAV systems. By utilizing a cryptographic consensus mechanism and peer-to-peer (P2P) networking infrastructure for message propagation and data transmission, blockchain allows all participants to maintain a transparent and immutable public distributed ledger. The decentralization provided by blockchain is promising for the mitigation of the impact of SPF and PBN by reducing the overhead of the central server in UAV networks. In addition, encryption algorithms, consensus protocols, and tamper-proof distributed ledgers of blockchain enhance the privacy and security of UAV networks. As a result, blockchain provides a "trust-free" network to guarantee the integrity, accountability, and traceability of UAV data. Furthermore, smart contracts (SC) introduce programmability into a blockchain to support a variety of customized business logic rather than classic P2P cryptocurrency transactions [9]. Therefore, blockchain is promising to enhance governance, regulation, and assurance in UAM networks with the help of decentralized security services, such as identification authentication [10], access control [11], and data validation [12].

The shift from centralized UAV networks to decentralized blockchain-assisted UAV systems improves the efficiency of system operations and ensures security and privacy guarantees. Existing blockchain-based UAV solutions mainly consider blockchain as a trusted network and immutable storage to improve the efficiency of communications [13,14], incentive mechanisms [15], security of access authentication [16,17], and data sharing processes [18,19]. However, directly adopting conventional blockchains to build decentralized UAV networks still meets tremendous challenges in IoD scenarios. The current solutions based on permissionless blockchains (e.g., Bitcoin [20] or Ethereum [21]) demand high computation resources in proof-of-work (PoW) mining processes such that they are not affordable to resource-constrained drones. While using permissionless blockchains such as Hyperledger [22] can achieve low energy consumption and high throughout, they are highly limited in terms of scalability and communication complexity.

To address the aforementioned limitations of integrating blockchain into UAV networks, this paper proposes LightMAN, a lightweight microchained fabric for data assurance and operation resilience-oriented UAM networks. Unlike existing works [6,8,18,19] that rely on computation-intensive PoW blockchains, LightMAN adopts microchain [23], a lightweight-designed blockchain, to achieve efficiency and security guarantees for a small-scale permissioned UAV network. As drone information and flight logs are securely and accurately stored on the immutable distributed ledger of the microchain, participants within a UAM network can verify the authenticity of drones and verify tamper-proof data sent to/from drones without relying on a third-party agency. Compared with blockchain-based UAV networks that either directly save raw data on the distributed ledger [18] or outsource raw data to a cloud server [19], our LightMAN allows encrypted data to be stored on a distributed data storage (DDS), while the microchain only records references of data as checkpoints. Such a hybrid on-chain and off-chain storage strategy not only improves performance (e.g., latency and throughput) but also ensures privacy preservation for sensitive information in UAM networks.

In brief, the key contributions of this paper are highlighted as follows:

(1) A complete LightMAN system architecture is presented along with details of key components and functionalities;
(2) A machine learning-based anomaly detection (MLAD) method to monitor the UAM networks in real time is proposed. To generate the source data (MAVLink message) for creating the cyber-resiliency scenario, we implemented a software-in-the-loop (SITL) simulator and associated demonstration package (pymavlink) in a python environment to emulate the message communications among UAVs;
(3) A lightweight blockchain called microchain is leveraged to guarantee security and privacy requirements in UAV data access and sharing scenarios; and
(4) A proof-of-concept prototype is implemented and tested on a small-scale physical network. The experimental results show that the proposed LightMAN only incurs less than two seconds of latency while committing transactions on the distributed ledger and no more than 18% overhead during access authentication.

The remainder of the paper is organized as follows: Section 2 provides background knowledge of UAV and blockchain technologies and reviews existing state-of-the-art blockchain-based UAV systems. Section 3 introduces the rationale and system architecture of LightMAN. Section 4 presents the prototype implementation, experimental setup, and performance evaluation. Finally, Section 5 summarizes this paper with a brief discussion on current limitations and future directions.

2. Background and Related Work

This section describes the fundamentals of the UAV concept, explains blockchain technology, and introduces the state-of-the-art decentralized solutions to secure UAM networks.

2.1. Unmanned Aerial Vehicles

Unmanned aerial vehicles (UAVs), simply called drones, are specific robotic IoTs, which have electronic components, mechanical power modules, and onboard operating systems to execute complicated tasks. According to their flying mechanisms, UAVs can be categorized as multi-rotor-wing drones, fixed-wing drones, and hybrid fixed/rotary-wing drones [24]. Regarding the range and altitude that a done can be remotely operated at, UAV platforms can be classified into two types: low-altitude platforms (LAPs) and high-altitude platforms (HAPs). Original UAVs were mainly used for battlefields, with advancements in hardware, software, and networking infrastructure, but there has been increasing usage of UAVs in civilian and commercial applications.

Owing to their unmanned nature and requirements for remote wireless communication, modern UAV-aided systems are vulnerable to different attacks [25]. Thus, the continued use of UAVs increases the need for cyber-awareness including UAVs in the airspace, the development of the automatic dependent surveillance broadcast (ADS-B), and the risk of cyber intrusion. The Federal Aviation Administration (FAA) mandates the national adoption of ADS-B, which uses “plaintext” to broadcast messages in avionics networks. Such an unencrypted ADS-B manner introduces serious privacy and security vulnerabilities, such as message spoofing for false aircraft position reports. As a result, current radar-based air traffic service (ATS) providers seek to preserve privacy and corporate operations of flight plans, position, and state data. Moreover, the privacy of aircraft track histories is mandatory and only accessible to authorized entities within UAM networks. In addition, it is necessary to ensure confidentiality, availability, and integrity for urban aircraft data accessing and sharing data during UAM operations.

2.2. Blockchain Technology

From the system architecture aspect, a typical blockchain system consists of three essential components: a distributed ledger, a consensus protocol, and smart contracts [26]. Essentially, distributed ledger technology (DLT) is a type of distributed database that is shared, replicated, and maintained by all participants under a P2P networking environment. Each participant maintains a local view of the distributed ledger in the context of a distributed computing environment, and a well-established consensus allows all participants to securely reach an agreement on a global view of the distributed ledger under consideration of failures (Byzantines or crash faults). Given different consensus algorithms and network models, distributed consensus protocols are categorized into Nakamoto consensus protocols [20] or Byzantine fault-tolerant (BFT) consensus protocols [27]. From a topology aspect, blockchain can be classified into three types: public (permissionless) blockchains, private (permissioned) blockchains, and consortium blockchains [28].

By using cryptographic and security mechanisms, a *smart contract* (SC) combines protocols with user interfaces to formalize and secure the relationships over computer networks [29]. Essentially, SCs are programmable applications containing predefined instructions and data stored at a unique address on the blockchain. Through exposing the public functions or application binary interfaces (ABIs), an SC acts as the trusted autonomous agent between parties to perform predefined business logic functions or contract agreements under specific conditions. Owing to the secure execution of predefined operational logic, unique addresses and public, exposed ABIs, using a SC provides an ideal decentralized app (Dapp) backbone to support upper-level IoT applications.

2.3. Blockchain-Based UAV Networks

There have been many studies in the past that have explored blockchain and smart contracts to enable decentralized UAV networks. In general, existing blockchain-based UAV networks can be categorized into three branches: securing UAV communications, maintaining data integrity and improving identity authentication.

2.3.1. UAV Communication

By utilizing the blockchain concept in the development of drone networks, a blockchain-empowered drone network called BeDrone allows drones in service to act as the miners of the blockchain [15]. Each drone can acquire computing and storage resources from nearby edge service providers to carry on the blockchain processes, such as mining blocks and storing ledgers. BeDrone uses game theory to design incentive mechanisms for resource allocation, acquisition, and trading among participants. However, details of the underlying blockchain framework are not discussed.

To ensure ultra-reliability and security for intelligent transport during drone-catching in multi-access edge computing (MEC) networks, a neural-blockchain-based transport model (NBTM) [13] was proposed by forming a distributed decision neural network for multiple blockchains. NBTM uses neural networks to formulate policies and rules as the drone-caching model for reliable communication and content sharing. A hierarchical blockchain model consisting of three blockchains and a master blockchain provides security mechanisms for content sharing and data delivery. The simulation results demonstrate that the proposed NBTM can enhance the reliability of UAV networks with a lower failure rate. However, the performance of using multi-blockchains is not mentioned.

To build agile and resilient UAV networks for the collaborative application of large-scale drone groups, a software-defined UAV network called SUV [30] was proposed by combining software-defined networking (SDN) and blockchain technology to achieve a decentralized, efficient and flexible network infrastructure. By decoupling the control panel and the data panel of a UAV network, SDN allows SUV to optimally manage all drones and simplify functions of data forwarding. Blockchain facilitates the decentralization of the SDN control panel and ensures the credibility of the SDN controller identity and behavior in an open networking environment. The proposed SUV is promising for the provision of flexibility, survivability, security, and programmability for 5G-oriented UAV networks [30]. However, its implementation and performance evaluation are not described.

Similar to the works [13,30] that focusesd on improving security in UAV communications, a lightweight blockchain based on a proof-of-traffic (PoT) consensus algorithm was proposed to provide secure routing for swarm UAVs [14]. PoT leverages the traffic status of swarm UAVs to construct a consensus rather than the computation resources used by PoW. The evaluation shows that PoT can reduce the burden of energy consumption and computational resource allocation for swarm UAV networking. However, the performance of PoT consensus is not discussed, such as transaction latency and throughput.

2.3.2. UAV Data Integrity

Some early works used blockchain as tamper-proof storage to protect the UAVs' data integrity during sharing and operating processes. To secure drone communications and preserve data integrity, a blockchain-based drone system called DroneChain [19] was proposed using a PoW blockchain and a cloud server. The collected data of each drone are associated with its device ID and are saved into a cloud server, while a hash of each data record is stored in the blockchain. DroneChain allows for data assurance, provenance, and resistance against tampering. Moreover, the distributed nature of DroneChain also improves the availability and resilience of data validation for potential failures and attacks. However, using a centralized cloud server for UAV raw data storage is prone to privacy violations and SPF in data querying and sharing.

To address issues of DroneChain that adopts the traditional cloud server and PoW blockchain in UAV networks, a secure data dissemination model based on a consortium blockchain was proposed for IoD [18]. All users and drones are divided into multiple clusters, and one master controller (MC) within a cluster can work as a normal node in a public Ethereum blockchain network. A forger node selection algorithm on the basis of utility function using game theory periodically selects one forger node for block generation. The experimental results evaluate the performance of the data dissemination model, such as the computation time of block creation and validation. However, details of blockchain design and data storage are not mentioned.

2.3.3. UAV Authentication

By storing identification and access control information in the distributed ledger, blockchain can provide decentralized authentication services for UAV networks. To solve issues of authentication of drones during flights, a secure authentication model with low latency for IoD in smart cities was proposed by using a drone-based delegated proof-of-stake (DDPOS) blockchain atop zone-based network architecture [16]. Similar to [18], a drone controller in each zone of a smart city is responsible for the management and authentication mechanism for drones, and it also handles all operations related to the blockchain. Compared to the original PoS algorithm, a customized DDPOS algorithm can mitigate mining centralization and the flaws of real-life voting in the UAV network. The experimental results show the efficiency of the proposed solution under a simulated environment, such as low package loss rate, high throughput, and end-to-end delay.

To address the challenges of centralized authentication approaches in cross-domain operations, a blockchain-based cross-domain authentication scheme for an intelligent 5G-enabled IoD was proposed [17]. The proposed solution uses a local private blockchain based on Hyperledger fabric to support drone registration and identity management. As multiple signatures based on threshold sharing are used to build an identity federation for collaborative domains, a smart contract contains access control policies, and multi-signatures aims to secure mutual authentication between terminals across different domains.

3. Design Rationale and System Architecture

UAM offers the potential to create a faster, cleaner, safer, and more integrated transportation systems. However, recent events have shown that modern UAVs are vulnerable to attack and subversion through faulty or sometimes malicious devices that are present on UAM communication networks, which increases the need for cyber awareness to include UAVs in the airspace and the risk of cyber intrusion. Aiming at a secure-by-design, intelligent and decentralized network architecture for assurance and resilience-oriented UAM networks, LightMAN leverages deep learning (DL) and microchains to enable efficient, secure, and privacy-preserving data access and sharing among participants in UAV networks. Figure 1 demonstrates the LightMAN architecture that consists of two sub-frameworks: (i) the UAM network and (ii) the microchain fabric.

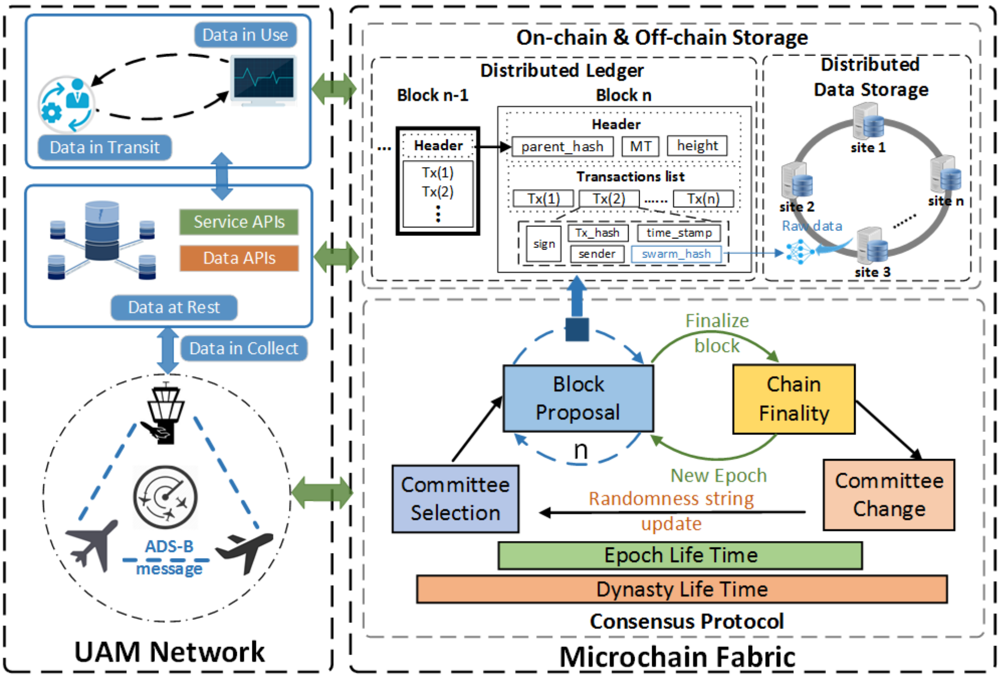

Figure 1. System Architecture of LightMAN.

A UAM network encompasses air traffic operations for manned and unmanned aircraft systems in a metropolitan area. The left part of Figure 1 shows a UAV application that provides on-demand, automated transportation services. Each drone uses its onboard sensors to enroll and capture raw mission data, such as ADS-B messages or MAVLink messages, and these data can be digitized and converted to key features, such as aircraft identification and trajectories. The operation centers (ground stations) can collect data for flight planning and monitoring. In addition, raw data can be transferred to an avionic data center that provides long-term storage services (data at rest) for high-level information fusion and analysis. Finally, a cloud server performs high-level computing extensive and big-data-oriented tasks such as multi-airborne collaborative planning and decision-making reasoning. Based on a thorough analysis of shared avionics data, intelligent avionic services (data in transit) incorporates AI technologies to optimize UAV services and protect against never-before-seen attacks. Information visualization (data in use) provides context-based human–machine interactions for authorized users to learn dynamic mission priorities and resource availability [31].

The microchain fabric acts as a security and trust networking infrastructure to provide decentralized security and privacy-preserving guarantees for UAM data. Microchain leverages a permissioned UAV network management and assumes that the system administrator is a trustworthy oracle to maintain registered identity profiles of UAM. Thus, each drone or user uses their unique ID to identify authentication and access control procedures. In addition, cryptographic primitives such as public key infrastructure (PKI) and encryption algorithms can guarantee the confidentiality and integrity of drone data (e.g., ADS–B) in communication. Moreover, microchain integrates a lightweight consensus protocol with a hybrid on-chain and off-chain storage to ensure UAV data and flight logs are stored securely and distributively without relying on any centralized server.

3.1. Deep Learning (DL)-Powered UAM Security

To better detect anomalous behaviors (e.g., aircraft route anomalies) to constantly collecti high-resolution cyber-attack information across avionics flight data, we have designed and developed DL-based cybersecurity monitoring techniques against cyber threats for UAM situation awareness (SAW). The developed LightMAN with cognitive-based decision support is not intended to replace human interaction and decision-making; rather, it is meant to support the operator to combine data, identify potential threats rapidly for a pre-planned mission, and provide timely recommended actions.

Learning directly from high-dimensional sensory inputs is one of the long-standing challenges. Our objective is to develop machine learning (ML)-based anomaly detection (MLAD) and reinforcement learning (RL) artificial agents that can achieve a good level of performance and generality on diagnostics and prognostics. Similar to a human operator, the goal for the agents is to learn strategies that lead to the greatest long-term rewards. Formally, MLAD can be described as a Markov decision process (MDP), which consists of s set of states, S, plus a distribution of starting states, $P(s_0)$; a set of actions, A; transition dynamics, $T(s_{t+1} \mid s_t, a_t)$, that map a state-action pair at time t to the distribution of states at time t + 1; a reward function, $R(s_t, a_t, s_{t+1})$; and a discount factor, $\delta \in [0,1]$, where smaller values place more emphasis on immediate rewards. It is assumed that an agent interacts with an environment, S, in a sequence of actions, actions, observations, and rewards. At each time-step, the agent selects an action, $a_t \in A, A = 1, \ldots, K$, which is passed to the environment and modifies its internal state and the corresponding reward [32]. In general, S may be stochastic. The system's internal state is not observable to the agent most of the time, instead, it observes various target features of interest from the environment, such as the signal features. It receives a reward R representing the change in overall system performance.

Based on the MLAD-RL strategy, we developed an automated monitoring mechanism for system-level source analytics. The monitoring data are defined as a set of metrics (e.g., route latitude/longitude, transmission delay, traffic buffer queue length, etc.) on each UAM edge and associated applications and processes. Given a large number of features, LightMAN uses feature extraction and reduction techniques in collected log data to select a set of the most critical features and implement deep learning-based detection schemes for identifying anomalous statuses. The general steps of the proposed anomaly monitoring technique are as follows: (i) *Data Collection*: The relevant sensory data collected across the system are assembled into a set of feature matrices. We define the feature as an individually measurable variable of the node being monitored (e.g., data frames, MAVLink messages, command and control (C2) mission logs, controller area network (CAN) buses, etc.); (ii) *Feature Extraction*: To effectively deal with high-dimensional data, we implement feature extraction techniques via named entity recognition (NER) [33] and the vector space model (VSM), which can reduce data dimensionality and improve analysis by removing inherent data dependencyl (iii) *Deep Learning-Based Detection*: LightMAN applies DL techniques (e.g., L-CNN, RNN/LSTM, etc.) to characterize the dynamic state of the monitored system. With the trained model in place, the operator can conduct the detection and classification of potential attacks.

As shown in Figure 2, the detection process consists of two main steps: the training process and the detecting process. In the training process, the collected log data are converted to a uniform data format for the learning process. We then train the classifier model for both normal and abnormal system states. In the online monitoring process, LightMAN monitoring tools collect real-time flight data, and the processed traffic data are sent to the learned classifier for anomaly detection. The effectiveness of the monitoring schemes is characterized by the true positive rate, false positive rate, monitoring time, overhead, etc.

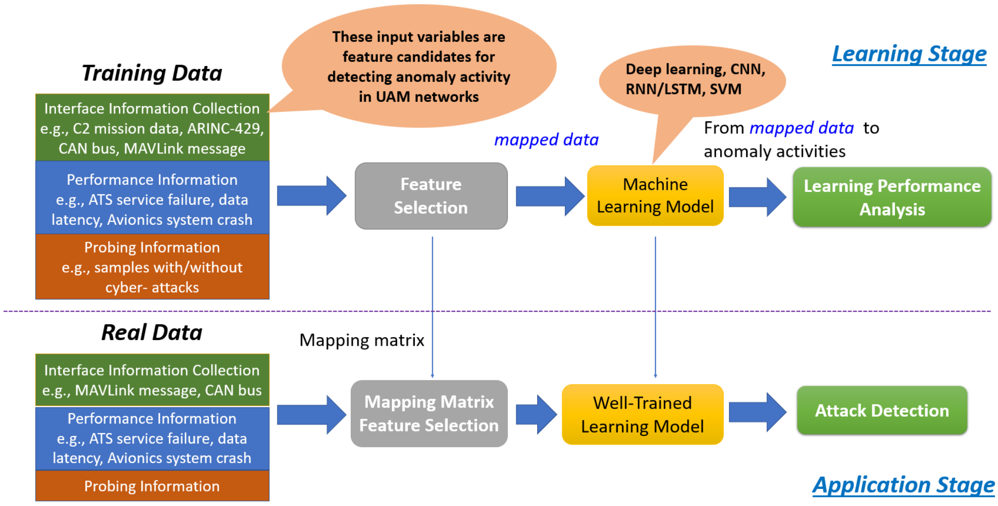

Figure 2. ML/DL Learning Process for UAM Monitoring.

3.2. Microchain Fabric for UAM Data Sharing

As the right part of Figure 1 shows, a microchain fabric consists of two sub-systems: (i) a lightweight consensus protocol that relies on a randomly selected consensus committee to achieve a low latency when committing transactions on the distributed ledger; (ii) a hybrid on-chain and off-chain storage strategy that improves efficiency and privacy-preservation. For details regarding the consensus protocol in the microchain, interested readers can refer to our earlier work [23,34]. The core functionalities and workflows are briefly described as follows:

- The lifetime of a committee is defined as a *dynasty*, and all nodes within the network use a random committee election mechanism to construct a new committee at the beginning of a new dynasty. The new committee members rely on their neighboring peers, which use a node discovery protocol to reach out to each other. Finally, all committee members maintain a fully connected consensus network, and non-committee nodes periodically synchronize states of the current dynasty. Until the current dynasty's lifetime is ending, committee members utilize an epoch randomness generation protocol to cooperatively propose a global random seed for the next committee election.
- Given a synchronous network environment, operations of consensus processes are coordinated in sequential rounds called *epochs*. The block proposal leverages an efficient proof-of-credit (PoC) algorithm, which allows the consensus committee to continuously publish blocks containing transactions and extend the main chain length. The block proposal process continues running multiple rounds until the end of an epoch. Then, a voting-based chain finality protocol allows committee members to make an agreement on a checkpointing block. As a result, temporary fork chains are pruned, and these committed blocks are finalized on the unique main chain.
- The organization of on-chain and off-chain storage is illustrated by the upper right part of Figure 1. As the basic unit of on-chain data recorded on the distributed ledger, a block contains header information (e.g., previous block hash and block height) and orderly transactions. The distributed data storage (DDS), which is built on a swarm [35] network, is used as off-chain storage. The UAV data and flight logs that require heterogeneous formats and various sizes are saved on the DDS, and they can be easily addressed by their swarm hash. In an optimal manner, each transaction only contains a swarm hash as a reference pointing to its raw data on the DDS. Compared with raw data, a swarm hash has a small and fixed length (32 or 64 bytes); therefore, all transactions have almost the same data size. It is promising to improve efficiency in transaction propagation without directly padding raw data into transactions.

4. Experimental Results and Evaluation

In this section, experimental configuration based on a proof-of-concept prototype implementation is described. Following that, we evaluate the performance of running LightMAN based on numerical results, which especially focus on microchain operations. Finally, a comparative evaluation among previous work highlights the main contributions of LightMAN in terms of lightweight blockchain design, performance improvement, security, and privacy properties.

4.1. Prototype Implementation

A proof-of-concept prototype of LightMAN was implemented and tested in a physical network environment. The microchain was implemented in Python with Flask [36] as a web-service framework. All security primitives such as digital signature, encryption algorithms, and hash functions were developed by using standard python library cryptography [37]. MAVLink [38] implemented a Software-In-The-Loop (SITL) simulator consisting of Pymavlink, ArduPilot, MAVProxy and QGroundControl. As a package of Python MAVLink libraries, Pymavlink was used to implement drone communication protocol and analyze flight logs. ArduPilot [39] is an open-source autopilot software that was used to simulate many drone types on a local server without any special hardware support. MAVProxy acted as the ground control station for ArduPilot, and QGroundControl provided the graphical user interface (GUI) for ArduPilot. We combined the SITL simulator and Pymavlink package to emulate UAM scenarios and collect MAVLink messages as UAV data.

Table 1 describes devices used for the experimental setup. Each validator of microchain was deployed on a Raspberry Pi (RPi) while a SITL simulator was deployed on the Redbarn HPC. The microchain test network contained 16 RPis. Regarding a test Swarm network, 6 service sites were deployed on six separate desktops that each had an Intel Core 2 Duo CPU E8400 @ 3 GHz and 4 GB of RAM. All devices were connected through a local area network (LAN).

Table 1. Configuration of Experimental Devices.

Device	Redbarn HPC	Raspberry Pi 4 Model B
CPU	3.4 GHz, Core i7-2600K (8 cores)	1.5 GHz, Quad core Cortex-A72 (ARM v8)
Memory	16 GB DDR3	4 GB SDRAM
Storage	500 GB HHD	64 GB (microSD card)
OS	Ubuntu 18.04	Raspbian GNU/Linux (Jessie)

4.2. MAVLink Message Data Acquisition

To better perform the machine learning-based anomaly detection (MLAD) within LightMAN among UAM networks, we leveraged the MAVLink Protocol, which stands for micro-air–vehicle link, and its related messages as our starting point for the security analysis of UAM networks. It is an open-source protocol, and it is supported by many closed-source projects for drones to send way-points, control commands, and telemetry data [40]. Usually, it contains two types of messages: state messages and command messages. State messages refer to these messages sent from the unmanned system to the ground station and contain information about the state of the system, such as its ID, location, velocity, and altitude. Command messages are usually sent from the ground station to the unmanned system to execute some actions by autopilot. Those messages are transmitted through WiFi, Ethernet, or other serial telemetry channels. We also utilized a SITL simulator (ArduPilot) [40] to emulate the MAVLink message communication. Specifically, we ran the ArduPilot directly on a local server without any special hardware. While running, the sensor data came from a flight dynamics model in a flight simulator.

Figure 3 presents an example of obtained MAVLink message source data. We recorded and saved this key information for MLAD training. For instance, *GPS_RAW_INT* refers to the absolute geolocation of GPS, latitude, longitude, and altitude. *AHRS* refers to the attitude and heading reference system (AHRS), which consists of sensors on three axes that provide attitude information for aircraft, including roll, pitch, and yaw. *EKF_STATUS_REPORT* indicates that an extended Kalman filter (EKF) algorithm was used to estimate vehicle position, velocity, and angular orientation based on rate gyroscopes, accelerometer, compass, GPS, airspeed, and barometric pressure measurements.

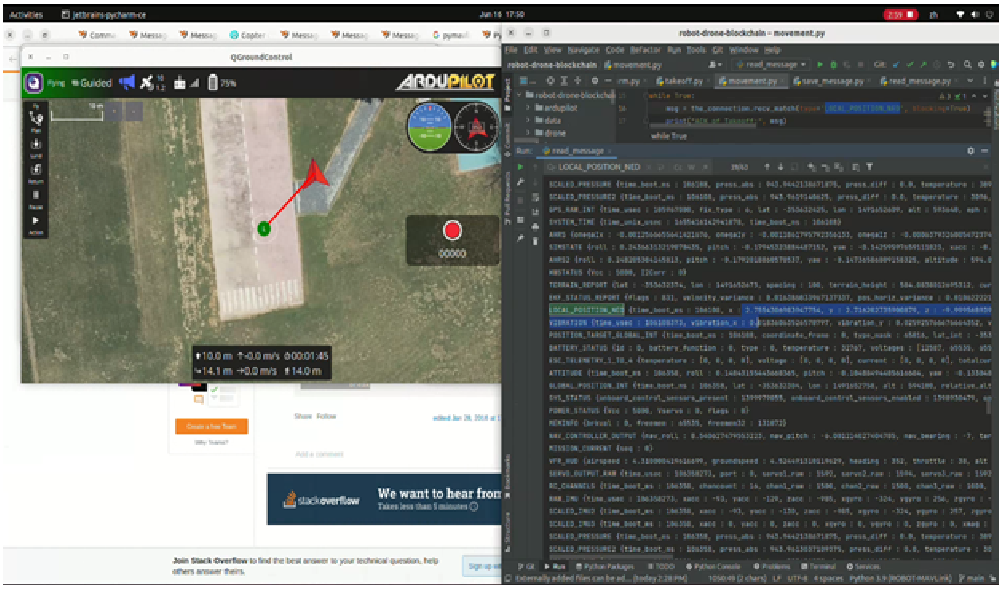

Figure 3. Software-In-The-Loop Simulation for Data Acquisition.

4.3. Performance Evaluation

During the identity authentication stage, the system administrator or data owners can launch a transaction to the microchain, which encapsulates a capability access token assigned to an entity. Then, any user can query such a token from microchain participants and verify it during the access validation process. We designed a capability-based access control (CapAC) scenario [11] in which one HPC simulates a service owner to record CapAC tokens into the microchain, and another RPi simulates a service provider to query CapAC tokens from the microchain for the access control process. We conducted 100 Monte Carlo test runs and used the average of results for evaluation.

4.3.1. End-to-End Latency of Authorizing Access Tokens

Figure 4 demonstrates how committee size K represented by the number of validators and access authorization transaction throughput Th_S measured by the transactions per second (tps) affects the end-to-end latency incurred by committing a transaction on a microchain network. As the microchain executes an efficient consensus protocol within a small consensus committee, it brings a lower total latency, which has marginal impacts for an increasing committee size K. As a trade-off, a small consensus committee containing resource-constrained RPi devices as validators has limited capability to process large volumes of transactions. Thus, the end-to-end latency is almost dominated by Th_S, as Figure 4 shows. We assume that each node within LightMAN waits no less than 5 s to collect UAV data and then launch a transaction. Thus, the network latency of committee transactions on microchain can satisfy real-time requirements of access authorization.

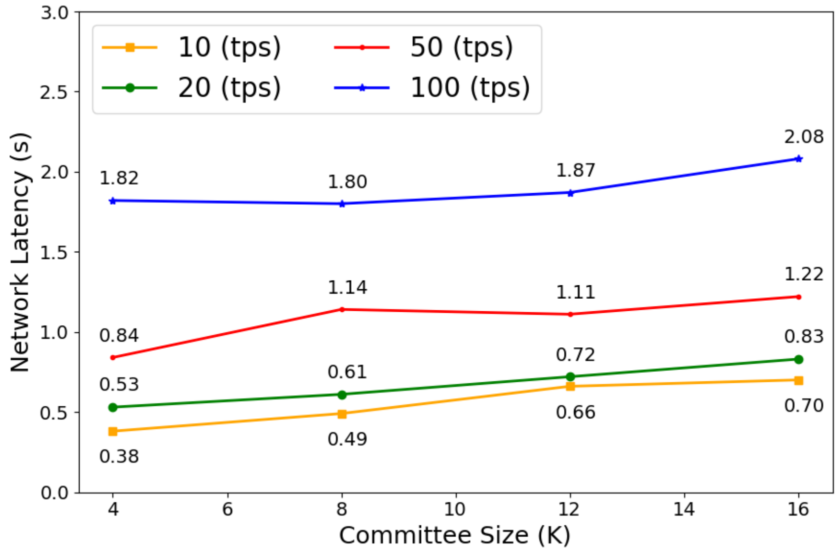

Figure 4. End-to-end latency of committing CapAC tokens on Microchain: committee size vs. tps.

4.3.2. Processing Time and Throughput in Access Authentication

For comparing our LightMAN's performance metrics with conventional centralized frameworks in access authentication, we designed basic scenarios as a benchmark, which did not cooperate with any access control strategy for UAV data access requests. To evaluate the processing time and throughput of access authentication operations, we used an HPC to simulate a cloud-based UAV server, which provided drone data query services given basic and LightMAN scenarios. Then, we let an RPi send multiple access requests to a UAV server and wait until all responses are correctly received.

Figure 5 shows average delays that evaluate how long a CapAC access request can be successfully handled by the UAV data server as increasing Th_S from 20 tps to 1000 tps. Regarding the fixed bandwidth of the test network, the capacity of UAV servers dominates the performance of handling access requests. Thus, the delays of access authentication are almost linear scale to Th_S given basic and LightMAN scenarios. However, LightMAN still demonstrates efficiency in the decentralized access authentication process that queries CapAC tokens from microchain and verifies access control policies, and it only incurred limited extra overheads (no more than 18%) compared with basic scenarios.

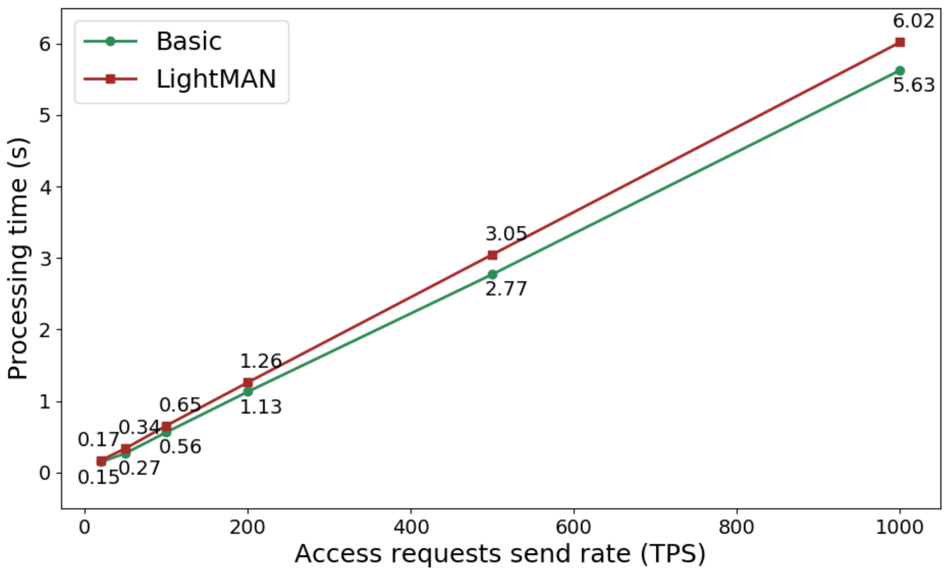

Figure 5. Processing Time of querying CapAC tokens and validating access rights.

To evaluate the data processing capability, we calculated throughput as $\frac{Th_S}{T_D}$, where T_D is the time latency of completing Th_S data tasks. A higher throughput indicates better system performance. Figure 6 presents the transaction throughput of handling access authentication requests, given that Th_S varies from 20 tps to 1000 tps. Each access request in LightMAN mode demands more computation resources on CapAC token validation; therefore, LightMAN demonstrates a lower transaction throughput than the basic mode even if the access request send rate Th_S is the same. Owing to system capacities, such as the network bandwidth and computation power of service providers, the transaction throughput of LightMAN and the basic mode become saturated under conditions where $Th_S \geq 500$ tps. Compared with the baseline, our solution can provide security and privacy features without significantly reducing system performance.

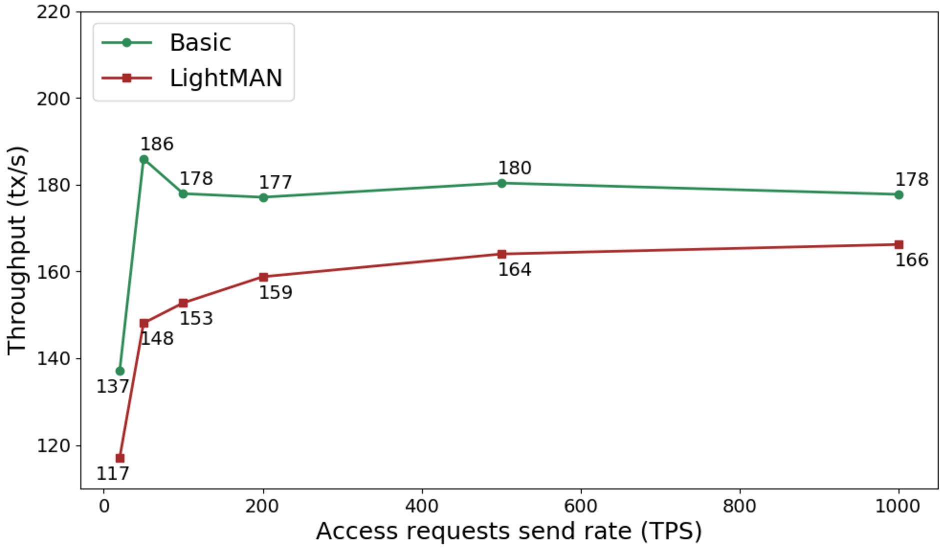

Figure 6. Throughput of querying CapAC tokens and validating access rights.

4.3.3. Computation Cost by Preserving Data Privacy

We assumed that MAVLink message data streams of a drone were encrypted and then recorded into DDS for each 60 s duration. As a result, each data file was about 1 MB, and we used these sample data files to evaluate computation overheads incurred by sharing UAV data via DDB along with data encryption and decryption procedures. Figure 7 shows the processing time of accessing data from Swarm and data encryption algorithms given different host platforms. Regarding DDS operations such as uploading files onto and downloading files from a private Swarm network, delays are almost the same on both platforms. Unlike downloading data, which simply query data from a DDS service site, uploading data onto DDS takes a longer time than is used to synchronize data units across distributed service sites within a Swarm network. Owing to constrained computation resources, RPi takes a longer process time to encrypt and decrypt data than the desktop does, even if sample data files have the same size. Compared with a 60 s cycle time of recording a drone's data, encrypting a data file and then uploading it onto DDS only brings marginal delays on both platforms (2.4 s on desktop and 3.2 s on RPi). Given data-in-use scenarios that frequently download files from a DDS service node and then decrypt them, the encryption algorithm incurs more computation overheads than Swarm operations. Given a data query request rate $Th_S = 500$ tps that takes an average of 3.05 s on access authentication, accessing UAV data incurs an extra 19% (0.57/3.05) of delays on desktop and 59% (1.79/3.05) of delays on RPi. As a trade-off, using encrypted data to protect private information is inevitable at the cost of a longer processing time.

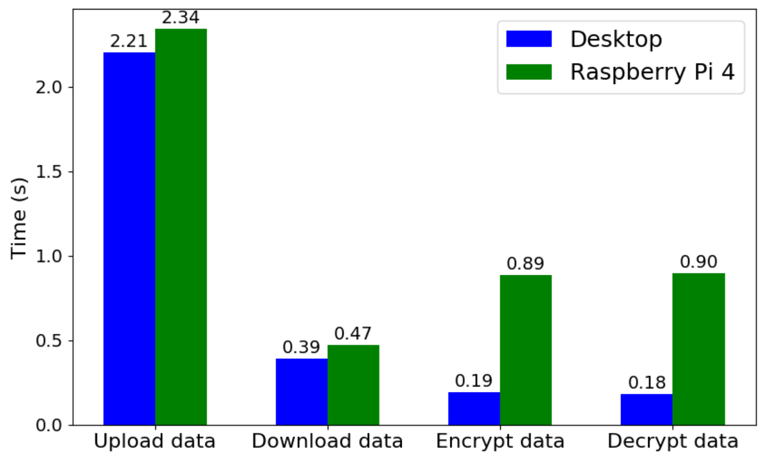

Figure 7. Processing time of data operations: accessing DDS and symmetric encryption.

4.4. Comparative Evaluation

Table 2 presents the comparison between our LightMAN and previous blockchain-based solutions for UAV networks. The symbol $\surd$ indicates that the scheme guarantees the security properties or implements some prototypes to evaluate the system performance or other specifications. The symbol $\times$ indicates the opposite case. Existing blockchain-based solutions that are developed to secure UAV communications [13–15] lack details on underlying blockchain frameworks, and most of them assumed that the cryptocurrency-oriented blockchain designs can be adopted in the UAV communication systems. Being fully aware of the specific performance requirements and resource constraints, we demonstrate a complete system architecture consisting of ML-based UAM monitoring and a lightweight microchain. Compared with solutions that adopt conventional PoW and BFT consensus protocols [17,19], LightMAN focuses on a lightweight blockchain design for IoD, which leverages a novel PoC+VCF consensus protocol to reduce computation and communication overheads on IoT systems. We especially evaluate blockchain performance (e.g., network latency, transaction throughput, and computation overheads) by applying a microchain-enabled security mechanism to access authentication and data sharing process scenarios, which are not considered or sufficiently discussed in related work [16,18].

In terms of the optimization for UAV data storage, a DDS is adopted atop the Swarm network as the off-chain storage to store raw UAV data. Therefore, LightMAN is promising for the enhancement of the system robustness (availability and recoverability) for data-sharing applications compared with existing solutions that rely on centralized storage [19]. Furthermore, LightMAN stores encrypted sensitive information on the DDS while only recording references of raw data on the transparent distributed ledger. As a result, blockchain transactions only contain references of small size rather than large volumes of UAV data. Such a hybrid on-chain and off-chain data storage structure not only reduces communication and storage overheads but also ensures privacy preservation in the data-sharing process by exposing hash-style references as proofs.

Table 2. Comparison among existing solutions.

	Consensus	Storage	Performance	Security	Privacy
BeDrone [15]	$\times$	$\times$	$\times$	$\surd$	$\times$
NBTM [13]	$\times$	$\times$	$\times$	$\surd$	$\times$
SwarmUAV [14]	PoT	$\times$	$\surd$	$\surd$	$\times$
DroneChain [19]	PoW	Centralized	$\surd$	$\surd$	$\times$
SecureIoD [18]	PoS	$\times$	$\times$	$\surd$	$\times$
ZoneIoD [16]	DDPoS	$\times$	$\surd$	$\surd$	$\times$
5G-IoD [17]	BFT	$\times$	$\surd$	$\surd$	$\times$
LightMAN	PoC+VCF	Decentralized	$\surd$	$\surd$	$\surd$

5. Conclusions and Future Work

This paper presents LightMAN, which combines DL-powered UAM security and a lightweight microchained fabric to support assurance and resilience-oriented UAM networks. The DL-based cybersecurity monitoring techniques can prevent cyber threats and provide cognitive-based decision support for UAM. A lightweight microchain works as a secure-by-design network infrastructure to enable decentralized security solutions for UAV access authentication and data sharing. The experimental results based on a prototype implementation demonstrate the effectiveness and efficiency of our LightMAN. However, there are open questions that need to be addressed before applying LightMAN to real-world UAM scenarios. We leave these limitations to our future work:

(1) Although the microchain is promising for providing a lightweight blockchain for a small-scale UAV network such as a drone cluster, it is not suitable for a large-scale UAM system demanding scalability and dynamicity in multidomain coordination. A hierarchical integrated federated ledger infrastructure (HIFL) [41] is promising for the improvement of scalability, dynamicity, and security for multi-domain IoD applications. Thus, our ongoing efforts include validating LightMAN in a real-world UAV network and investigating the integration of microchain and HIFL to support secure inter-chain transactions in a large-scale UAM system.

(2) There are still unanswered questions regarding an incentive mechanism that motivates users and drones to devote their resources (e.g., computation, storage, and networking) to participant consensus processes and gain extra profits. In our future work, we will use game theory to model incentive strategies and evaluate the effectiveness, security, and robustness of LightMAN in IoD scenarios.

(3) The third important milestone is an in-field validation of LightMAN in the context of practical applications. Once all the functional blocks and integrated systems are successfully tested in the lab environment, a small-scale drone network will be created with drones that are designed by the team. The completely customized drones will allow us to mount the LightMAN system on top of multiple application-determined sensing blocks, such as smart surveillance cameras or motion sensors. Specifically, to better validate the effectiveness of LightMAN, we plan to test our implementation with a hardware-in-the-loop (HITL) design in a hierarchical practical environment. We will deploy our validator devices on the hardware drones and establish a small-scale decentralized platform. Each drone will function as an individual node with communication protocols (e.g., MAVLink, TCP/IP) within LightMAN. Some typical communication-related anomalies (e.g., GPS spoofing, and channel access attacks) will be crafted to perform a practical injection attack onto the device sensors. In the future study, we will also build multiple clients and servers onboard to stream the shared data (e.g., MAVLink messages) and process the UAM monitoring among UAVs in real time.

Author Contributions: Conceptualization, R.X., S.W., Y.C., G.C. and K.P.; methodology, R.X., S.W. and Y.C.; software, R.X. and S.W.; validation, R.X., S.W. and Y.C.; formal analysis, R.X., S.W. and Y.C.; funding acquisition, Y.C.; investigation, R.X., S.W. and Y.C.; resources, R.X., S.W. and G.C.; data curation, R.X. and S.W.; writing—original draft preparation, R.X., S.W. and Y.C.; writing—review and editing, R.X., S.W. and Y.C.; visualization, R.X. and S.W.; supervision, Y.C.; project administration, Y.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research was partially funded by the United State National Science Foundation (NSF) under the grant CNS-2141468.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors want to thank Erik Blasch for his guidance and suggestions during the writing of this manuscript. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Air Force Research Laboratory or the U.S. government.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

ABI	Application Binary Interfaces
AC	Access Control
ADS-B	Automatic Dependent Surveillance Broadcast
AI	Artificial Intelligence
ATS	Air Traffic Service
CAN	Controller Area Network
CapAC	Capability-based Access Control
DApp	Decentralized App
DDS	Distributed Data Storage
DDoS	Distributed Denial-of-Service
DL	Deep Learning
DLT	Distributed Ledger Technology
IoD	Internet of Drones
IoT	Internet of Things
MC	Master Controller
MEC	Multi-Access Edge Computing
ML	Machine Learning
PBN	Performance Bottleneck
PoC	Proof-of-Credit
PoT	Proof-of-Traffic
PoW	Proof-of-Work
PKI	Public Key Infrastructure
QoE	Quality-of-Experience
QoS	Quality-of-Service
RL	Reinforcement Learning
SAW	Situational Awareness
SC	Smart Contract
SDN	Software-defined Networking
SITL	Software-In-The-Loop
SPF	Single Point of Failure
UAM	Urban Air Mobility
UAV	Unmanned Aerial Vehicle

References

1. Xu, R.; Nikouei, S.Y.; Nagothu, D.; Fitwi, A.; Chen, Y. Blendsps: A blockchain-enabled decentralized smart public safety system. *Smart Cities* **2020**, *3*, 928–951. [CrossRef]
2. Xu, R.; Lin, X.; Dong, Q.; Chen, Y. Constructing trustworthy and safe communities on a blockchain-enabled social credits system. In Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, New York, NY, USA, 5–7 November 2018; pp. 449–453.
3. Alladi, T.; Chamola, V.; Sahu, N.; Guizani, M. Applications of blockchain in unmanned aerial vehicles: A review. *Veh. Commun.* **2020**, *23*, 100249. [CrossRef]
4. Hassija, V.; Chamola, V.; Agrawal, A.; Goyal, A.; Luong, N.C.; Niyato, D.; Yu, F.R.; Guizani, M. Fast, reliable, and secure drone communication: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 2802–2832. [CrossRef]
5. Chen, N.; Chen, Y.; Blasch, E.; Ling, H.; You, Y.; Ye, X. Enabling smart urban surveillance at the edge. In Proceedings of the 2017 IEEE International Conference on Smart Cloud (SmartCloud), New York, NY, USA, 3–5 November 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 109–119.
6. Han, T.; Ribeiro, I.D.L.; Magaia, N.; Preto, J.; Segundo, A.H.F.N.; de Macêdo, A.R.L.; Muhammad, K.; de Albuquerque, V.H.C. Emerging drone trends for blockchain-based 5G networks: Open issues and future perspectives. *IEEE Netw.* **2021**, *35*, 38–43. [CrossRef]

7. Aloqaily, M.; Bouachir, O.; Boukerche, A.; Al Ridhawi, I. Design guidelines for blockchain-assisted 5G-UAV networks. *IEEE Netw.* **2021**, *35*, 64–71. [CrossRef]
8. Blasch, E.; Xu, R.; Chen, Y.; Chen, G.; Shen, D. Blockchain methods for trusted avionics systems. In Proceedings of the 2019 IEEE National Aerospace and Electronics Conference (NAECON), Dayton, OH, USA, 15–19 July 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 192–199.
9. Xu, R.; Zhai, Z.; Chen, Y.; Lum, J.K. BIT: A blockchain integrated time banking system for community exchange economy. In Proceedings of the 2020 IEEE International Smart Cities Conference (ISC2), Piscataway, NJ, USA, 28 September–1 October 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–8.
10. Xu, R.; Chen, Y.; Blasch, E.; Chen, G. Exploration of blockchain-enabled decentralized capability-based access control strategy for space situation awareness. *Opt. Eng.* **2019**, *58*, 041609. [CrossRef]
11. Xu, R.; Chen, Y.; Blasch, E.; Chen, G. Blendcac: A smart contract enabled decentralized capability-based access control mechanism for the iot. *Computers* **2018**, *7*, 39. [CrossRef]
12. Nikouei, S.Y.; Xu, R.; Nagothu, D.; Chen, Y.; Aved, A.; Blasch, E. Real-time index authentication for event-oriented surveillance video query using blockchain. In Proceedings of the 2018 IEEE International Smart Cities Conference (ISC2), Kansas City, MO, USA, 16–19 September 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–8.
13. Sharma, V.; You, I.; Jayakody, D.N.K.; Reina, D.G.; Choo, K.K.R. Neural-blockchain-based ultrareliable caching for edge-enabled UAV networks. *IEEE Trans. Ind. Inform.* **2019**, *15*, 5723–5736. [CrossRef]
14. Wang, J.; Liu, Y.; Niu, S.; Song, H. Lightweight blockchain assisted secure routing of swarm UAS networking. *Comput. Commun.* **2021**, *165*, 131–140. [CrossRef]
15. Chang, Z.; Guo, W.; Guo, X.; Chen, T.; Min, G.; Abualnaja, K.M.; Mumtaz, S. Blockchain-empowered drone networks: Architecture, features, and future. *IEEE Netw.* **2021**, *35*, 86–93. [CrossRef]
16. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Karimipour, H.; Srivastava, G.; Aledhari, M. Enabling drones in the internet of things with decentralized blockchain-based security. *IEEE Internet Things J.* **2020**, *8*, 6406–6415. [CrossRef]
17. Feng, C.; Liu, B.; Guo, Z.; Yu, K.; Qin, Z.; Choo, K.K.R. Blockchain-based cross-domain authentication for intelligent 5G-enabled internet of drones. *IEEE Internet Things J.* **2021**, *9*, 6224–6238. [CrossRef]
18. Aggarwal, S.; Shojafar, M.; Kumar, N.; Conti, M. A new secure data dissemination model in internet of drones. In Proceedings of the 2019 IEEE International Conference on Communications (ICC 2019), Shangai, China, 20–24 May 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–6.
19. Liang, X.; Zhao, J.; Shetty, S.; Li, D. Towards data assurance and resilience in IoT using blockchain. In Proceedings of the 2017 IEEE Military Communications Conference (MILCOM 2017), Baltimore, MD, USA, 23–25 October 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 261–266.
20. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Decentralized Business Review. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 20 October 2022).
21. Welcome to Ethereum. Available online: https://ethereum.org/en/ (accessed on 30 August 2022).
22. Hyperledger Fabric. Available online: https://hyperledger-fabric.readthedocs.io/en/latest/ (accessed on 30 July 2022).
23. Xu, R.; Chen, Y.; Blasch, E. Microchain: A Light Hierarchical Consensus Protocol for IoT Systems. In *Blockchain Applications in IoT Ecosystem*; Springer: Cham, Switzerland, 2021; pp. 129–149.
24. Fotouhi, A.; Qiang, H.; Ding, M.; Hassan, M.; Giordano, L.G.; Garcia-Rodriguez, A.; Yuan, J. Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3417–3442. [CrossRef]
25. Blasch, E.; Sabatini, R.; Roy, A.; Kramer, K.A.; Andrew, G.; Schmidt, G.T.; Insaurralde, C.C.; Fasano, G. Cyber awareness trends in avionics. In Proceedings of the 2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC), San Diego, CA, USA, 8–12 September 2019; pp. 1–8.
26. Xu, R.; Nagothu, D.; Chen, Y. Decentralized video input authentication as an edge service for smart cities. *IEEE Consum. Electron. Mag.* **2021**, *10*, 76–82. [CrossRef]
27. Lamport, L.; Shostak, R.; Pease, M. The Byzantine generals problem. *ACM Trans. Program. Lang. Syst.* **1982**, *4*, 382–401. [CrossRef]
28. Ferrag, M.A.; Derdour, M.; Mukherjee, M.; Derhab, A.; Maglaras, L.; Janicke, H. Blockchain technologies for the internet of things: Research issues and challenges. *IEEE Internet Things J.* **2018**, *6*, 2188–2204. [CrossRef]
29. Szabo, N. Formalizing and securing relationships on public networks. *First Monday* **1997**, *2*. [CrossRef]
30. Hu, N.; Tian, Z.; Sun, Y.; Yin, L.; Zhao, B.; Du, X.; Guizani, N. Building agile and resilient UAV networks based on SDN and blockchain. *IEEE Netw.* **2021**, *35*, 57–63. [CrossRef]
31. Blasch, E.; Raz, A.K.; Sabatini, R.; Insaurralde, C.C. Information Fusion as an Autonomy enabler for UAS Traffic Management (UTM). In Proceedings of the AIAA Scitech Forum 2021, Virtual Event, 11–15 January 2021; pp. 1–12.
32. Mnih, V.; Kavukcuoglu, K.; Silver, D.; Graves, A.; Antonoglou, I.; Wierstra, D.; Riedmiller, M.A. Playing Atari with Deep Reinforcement Learning. *arXiv* **2013**, arXiv:1312.5602.
33. Li, J.; Sun, A.; Han, J.; Li, C. A Survey on Deep Learning for Named Entity Recognition. *IEEE Trans. Knowl. Data Eng.* **2020**, *34*, 50–70. [CrossRef]
34. Xu, R.; Chen, Y. μDFL: A Secure Microchained Decentralized Federated Learning Fabric atop IoT Networks. *IEEE Trans. Netw. Serv. Manag.* **2022**, *19*, 2677–2688. [CrossRef]

35. Swarm. Available online: https://ethersphere.github.io/swarm-home/ (accessed on 30 September 2022).
36. Flask: A Pyhon Microframework. Available online: https://flask.palletsprojects.com/ (accessed on 30 September 2022).
37. Pyca/Cryptography Documentation. Available online: https://cryptography.io/ (accessed on 30 September 2022).
38. MAVLink Developer Guide. Available online: https://mavlink.io/en/ (accessed on 30 September 2022).
39. ArduPilot Project. Available online: https://github.com/ArduPilot/ardupilot (accessed on 30 September 2022).
40. Taylor, M.; Chen, H.; Qin, F.; Stewart, C. Avis: In-Situ Model Checking for Unmanned Aerial Vehicles. In Proceedings of the 2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Taipei, Taiwan, 21–24 June 2021.
41. Xu, R.; Chen, Y.; Li, X.; Blasch, E. A Secure Dynamic Edge Resource Federation Architecture for Cross-Domain IoT Systems. In Proceedings of the 2022 International Conference on Computer Communications and Networks (ICCCN), Waikiki Beach, Honolulu, HI, USA, 25–27 July 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–8.