A Cybersecurity Service for UAS Traffic Management: Development and Field Testing

Sarah Lee, Michael Ades, Oscar Montealegre, Kevin Lei, Jaewon Kim, Sandip Roy
Texas A&M University, College Station, TX 77845, USA

Abstract – A cybersecurity service is developed for managed high-density Uncrewed Aircraft System (UAS) operations in airspace volumes, including future operations governed by UAS Traffic Management (UTM) capabilities. The service comprises four primary functions—context-aware authentication and authorization, Security Information and Event Management (SIEM), policy-based cyber defense, and targeted encryption—each customized for the UTM context and integrated into a modular service for UAS operations. Special emphasis is placed on the SIEM function, which leverages mission and operational context to distinguish between trusted and untrusted UASs, enabling real-time detection and response to cyber threats. The backend adopts a hybrid data architecture, separating authoritative operational information from high-volume telemetry and analytics to enhance both operational resilience. The cybersecurity service has been instantiated in a laboratory environment, and initial testing has been conducted with a focus on attestation and identity management.

I. Introduction

A substantial effort is underway to normalize complex Uncrewed Aircraft System (UAS) operations within the airspace. In particular, in the United States, the Federal Aviation Administration has recently proposed a rule to normalize Beyond Visual Line-of-Sight (BVLOS) operations in large swaths of low-altitude airspace [9]. Even more complex operations, such as operations near airports/vertiports or in congested high-altitude airspace and very high density operations using UAS swarms are envisioned in the future. Similar efforts to enable routine UAS operations within the aviation system are underway in Europe, Canada, the Middle East, and elsewhere.

Routine UAS operations within complex airspace volumes will require a comprehensive infrastructure which includes communication networks, ground- and air- technology assets, facilities, data services, and human personnel. The operations will also involve multiple UASs and crewed aircraft, and may be subject to various disruptors (terrain/weather, birds, unauthorized UASs, cyber threats). Ensuring the security of the operations against heterogeneous threats is therefore critical for the management of risk, and at the same time is a substantial challenge. There is a recognition, in particular, that cyber threats are a substantial concern both because of their likelihood/frequency, and the potential for systemic impacts. As an example, the proposed FAA rule for normalized BVLOS operations explicitly requires: 1) cyber policy implementation to protect operations against cyber threats; and 2) real-time detection, mitigation, and data collection for attacks. Future operations with even higher complexity/risk are likely to have even more stringent cybersecurity requirements.

A limited number of recent studies have begun to examine cyber-security for complex UAS operations that are integrated in the airspace system. In this direction, the important study by Sampigethaya and Kopardekar gives a comprehensive overview of the specific needs, issues, and potential technologies for cybersecurity of complex UAS operations in the airspace, with a focus on low-altitude operations involving many small UASs (often referred to as UAS Traffic Management or UTM) [1]. More recent studies have begun to envision frameworks for cyber defense,

considered more expansive operational scenarios beyond UTM, and undertaken simulations of cyber attack impacts [2-4]. In our recent work, we also proposed and architected an indoor testbed for assessing cyber attacks/defenses to multi-UAS operations through flight tests [5]. These various studies highlight special characteristics of airspace-integrated UAS operations that make cybersecurity challenging (e.g., the increased democratization of access creating susceptibility, the potential physical-world consequences of both threats and remediations, the reliance on domain-specific protocols, etc). These studies on the cybersecurity of UAS operations are a part of a broader effort to manage cyber threats to the aviation system as a whole, which has been increasingly disrupted by cyber attacks and failures [6,7]. There is also an important complementary line of work that considers the cybersecurity of individual UASs, and their communication links with operators [8,10-12].

Despite the growing interest in UAS operations cybersecurity, to our knowledge, there has not yet been an effort to develop a customized, generally-usable toolset or service for cybersecuring UAS operations in the airspace. Our team has architected and pursued initial implementation/testing of such a cybersecurity service for UAS operations in airspace volumes, with a focus on supporting complex multi-UAS operations requiring UTM (e.g., operations governed by the proposed FAA rule for normalized BVLOS operations). Our service aims to comprehensively address cyber defense needs, including authentication and authorization of UASs and other assets, security information and event management, response/mitigation for breaches, and targeted encryption of communications on demand. It is also structured as a modular service that can be easily added on to existing airspace management functions, making its integration into airspace operations practical. The primary goal of this article is to scope and report on the developed cybersecurity service. The instantiation and initial testing of the service in our indoor UTM environment is also discussed.

The article is organized as follows. The capabilities provided by the cybersecurity service, and their position within the UAS operations/management framework, are presented in Section II. The architecture and details of the cybersecurity service are described in Section III. An initial effort to instantiate and test the service in our laboratory is discussed in Section IV.

II. Capabilities Provided by the Cybersecurity Service

A framework for the management of UAS operations within airspace volume(s) is shown in Figure 1, and the cybersecurity functions or capabilities provided by our service are overlaid on top of the framework.

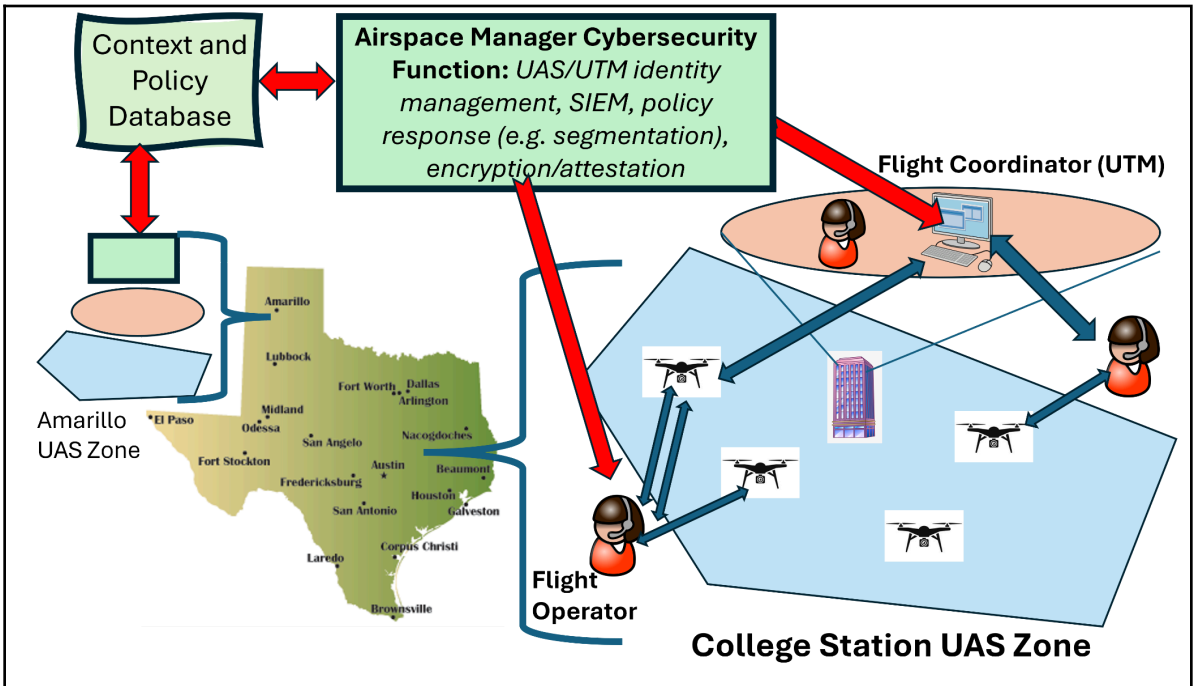

Figure 1: *Illustration of the scope and functions provided by our cybersecurity service (green boxes), overlaid on a diagram of multi-UAS operations in selected airspace volumes.*

The architecture considers *managed* multi-UAS operations within one or more low- to medium- altitude airspace volumes, which may include manually-operated UASs within visual line-of-sight, manually-operated UASs beyond visual line-of-sight, and potentially automated or group-controlled UAS. Vehicle operators provide command signals and get data from the UASs via a communication network, which may be of various types (e.g., a simple radio-control link, a local wireless or cellular network, or a satellite communication network). Centralized management of traffic operations by an authority, which we refer to as the *airspace manager,* is assumed. The airspace manager is responsible for ensuring that multi-UAS operations are safe, using various data-based services including surveillance, strategic or tactical deconfliction, detect-and-avoid, conformance monitoring, deconfliction with crewed aircraft using ADS-B, etc. For low-altitude operations considered in the new FAA rule, it is anticipated that airspace management for a given airspace volume will be provided by a commercial flight coordinator, which may be a major flight operator or may be an independent entity (see Figure 1). In this context, the airspace manager for an airspace volume handles a suite of services for UAS traffic management (UTM), and has the ability to communicate with the UAS operators and perhaps the UASs themselves. The airspace manager also has the authority to regulate traffic, either through communication with flight operators or perhaps direct command to the UASs themselves. For the operations considered in the proposed FAA rule, UTM services are provided by Automated Data Service Providers (ADSPs), The UTM service may also leverage other ground or air assets (e.g., sensors), which communicate with the UTM capability. Multi-UAS operations beyond the scope of the FAA rule (e.g., operations at higher altitudes, military operations) may have somewhat varied authorities and operational frameworks, but typically would involve management by a major flight operator or flight coordinator.

A multi-functional cybersecurity service is developed to protect managed multi-UAS operations in airspace volumes against cyber-initiated attacks and failures, see green boxes in Figure 1. The core of the solution is the *Airspace Manager Cybersecurity Function,* which provides multiple cybersecurity functions or capabilities to the airspace manager. The service comprises four customized capabilities, which are listed in the Airspace Manager Cybersecurity Function box. The four functions are: 1) authentication and authorization, 2) security information and event management (SIEM), 3) context-aware policy-based response to cyber events (e.g. using network-based defenses such as segmentation), and 4) targeted additional encryption. The Airspace Manager Cybersecurity Function for each airspace region also connects to a global Context and Policy Database, which maintains authoritative global information (e.g., hardware-backed UAS identities, attack signatures, global policies). The cybersecurity service is itself envisioned as a data service for UTM or, more broadly, airspace management; in the scope of the FAA rule, we envision the cybersecurity service as being provided by an ADSP. The global database is envisioned as cloud-based, which the airspace-manager-functions may be either hosted at the manager's facilities or on the cloud.

In the rest of this section, we briefly overview the four main cybersecurity capabilities or functionalities provided by our service; the architecture and details of the service are described in the following Section IV. Here are the overviews of the capabilities:

1. Authentication and Authorization: The authentication and authorization service is responsible for identity and access management for UASs (primary), and also potentially for human personnel (drone operators, managers/coordinators) and fixed assets like ground surveillance (collectively called endpoints). Specifically, the capability allows continuous attestation of assets involved in the airspace volume as a precursor to communication/command, and then supports trust-based identity verification for the assets as part of the event-management pipeline. Authentication is based on public-key (asymmetric) cryptography, which may be hardware-backed. In addition, the capability distinguishes trusted and untrusted assets in a customized context-informed way; these distinctions are used to manage communication/control access to ensure safety in emergency and nonemergency scenarios while also meeting cybersecurity requirements. Dynamic protocols for re-authentication are also included through a lease-based system.

2. Security Information and Event Management

The Security Information and Event Management (SIEM) function capability permits comprehensive logging and display-on-command of cyber data from assets. The core of the capability is a multi-faceted cyber anomaly/intrusion detection tool. The tool encompasses text-based search of logs, as well as signature-based detection of anomalies in spatiotemporal data (surveillance data, etc). The novelty of the detection capability is the use of customized anomaly signatures and detection mechanisms, tailored specifically for complex UAS operations. Event alarming for airspace

coordinators/managers is also performed.

3. Response
The authentication & authorization function, as well as the SIEM function, feed into a cyber defense or response capability. The cyber-defense capability is designed to use context-specific policies to determine a response action, and then to implement the action using a range of tools. For example, network-based defenses, based on granular network segmentation technologies, can be used to isolate or restrict UAS communications with the goal of minimizing threat impacts. The novelty in the cyber defense solution lies in the use of aviation-context-aware defenses that recognize safety constraints. Adaptation of responses to changing contexts is also a design goal. We note that the response function is only partly architected and developed, and hence modification is expected in the future.

4. Targeted Encryption
Encryption of communications for managed UAS operations is complicated to operationalize, given the variety of communication media, protocols, and device types that may be used. Our cybersecurity service allows for targeted encryption, per the needs of the airspace manager. Lightweight encryption based on Datagram Transport Layer Security (DTLS) can be enabled for specialized communications, such as those that use Mavlink.

III. Cybersecurity Service Architecture and Details

The cybersecurity service's architecture is designed to support continuous contest-aware trust assessment, anomaly detection, and cyber threat response in multi-UAS environments, with the goal of achieving the capabilities described in Section II. The design specifically enables cyber defense for UAS operations by integrating attestation, SIEM analytics, and policy-driven mitigation, in a way that is cognizant of and appropriately constrained for safety- and time- critical airspace operations. Figure 2 presents the integrated system architecture for our solution, illustrating how Remote Attestation (RATS), distributed SIEM capabilities, and a hybrid data architecture collectively enable real-time cyber threat detection and response in multi-UAS operations. The architecture is meant to flexibly support proposed UAS operational frameworks with limited additional hardware/software and no modifications to core airspace operations. Specifically, the architecture is designed to allow airspace managers (flight coordinators or key flight operators) which can communicate with airspace UASs or other assets to seamlessly conduct identity management and cyber threat detection. Further, the architecture allows direct enactment of policy responses through commands to UASs when this is allowed, or alternatively indirect enactment of policy through coordination with flight operators otherwise.

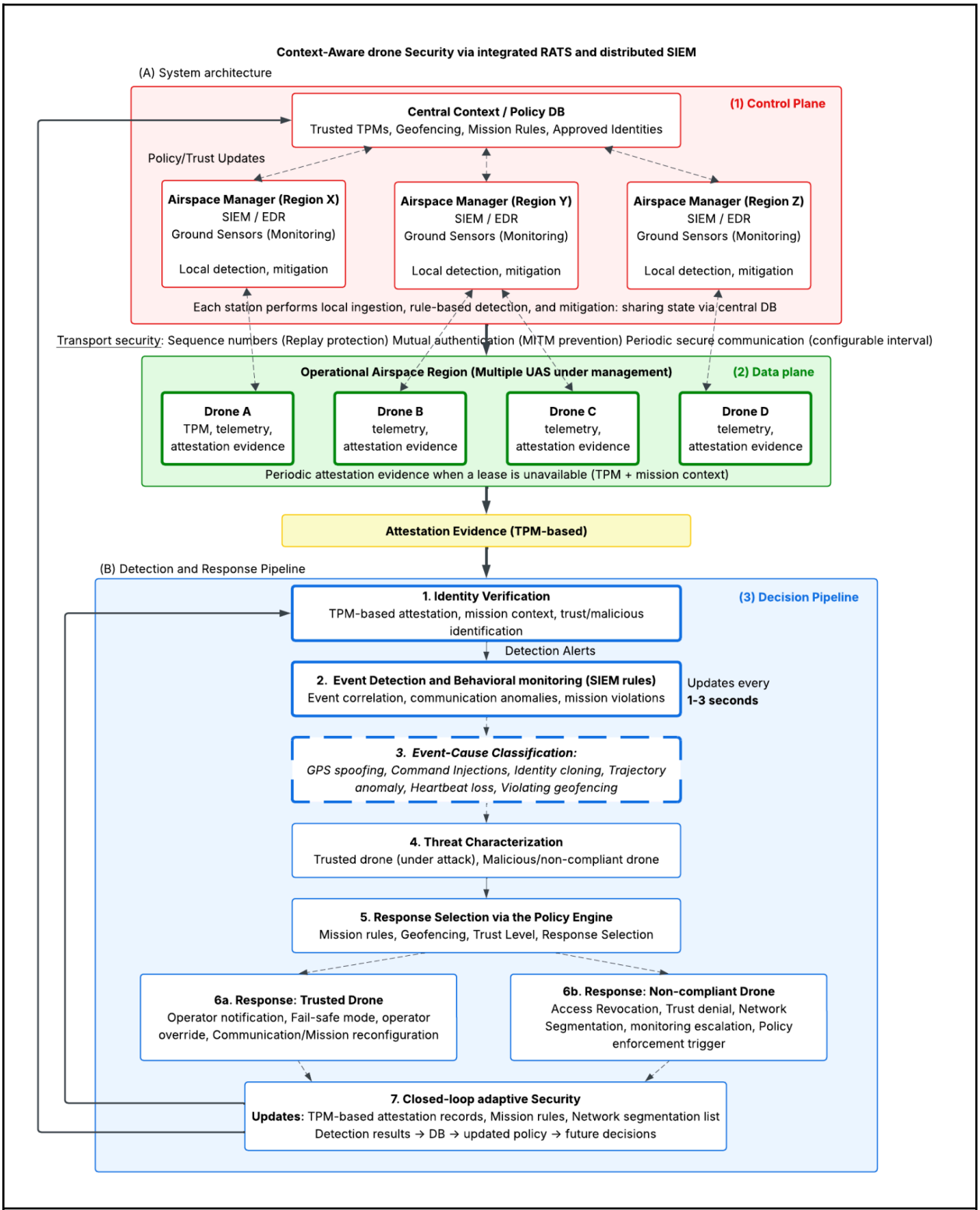

Figure 2: *Context-aware cybersecurity architecture for UAS Traffic Management (UTM), illustrating how airspace managers perform continuous identity verification, anomaly detection, and mission-aware response for drones operating within defined airspace regions.*

A. Overview of the Multi-Layer Architecture and Workflow:

The architecture is defined in two layers (see Figure 2): a control plane which manages authoritative airspace

cyber-operations states and policies (e.g., UAS identities, signatures of potential attacks, rules for addressing threats), and processes this information along with ingested telemetry for decision-support; and a data plane which is responsible for collecting high-volume telemetry. This distinction simplifies scalable deployment, verification, and compliance in complex UAS Traffic Management (UTM) environments by separating authoritative policy state from high-volume telemetry, thereby enabling deterministic decision-making, verifiable audit trails, and traceable enforcement actions necessary for regulatory compliance and safety assurance.

The control plane is itself a hierarchical entity. It is anchored by a centralized cloud-based Context and Policy Database, implemented using ScyllaDB, which maintains: 1) trusted system state, including UAS identities derived from hardware roots of trust, global mission and airspace context, cyber attack signatures, and geofencing constraints; and 2) global policy requirements (e.g., isolation procedures for potentially compromised UASs). Geofencing constraints are maintained as part of the authoritative control-plane state and distributed to Airspace Manager nodes, where they are locally cached and used by the SIEM backend for low-latency, context-aware anomaly detection and policy enforcement. Beyond static storage, the database actively supports authentication and authorization by incorporating updates from behavioral anomaly detection and SIEM-derived insights, enabling dynamic refinement of trust and access control decisions across the system.

In addition, the control plane includes an Airspace-Manager Cybersecurity Function for each managed airspace volume. The Airspace Manager Cybersecurity Function is a software module available for use by an authority or authorities responsible for UAS traffic in the airspace volume and able to communicate with UASs in the volume. The function typically would be hosted by an airspace/flight coordinator and/or a major flight operator, collectively referred to as an Airspace Manager. Geofencing constraints are defined within the centralized control-plane database and propagated to Airspace Manager nodes, where they are cached locally and incorporated into SIEM-based detection logic for real-time, context-aware evaluation. The Airspace Manager Cybersecurity Function implements context-aware identity management, SIEM, and policy-based response, using stored information from the Context and Policy Database together with cyber telemetry from UASs and airspace sensors. This distributed structure allows scalable global management of identities/threats and ensures global consistency in policy enforcement, while also supporting customized distributed decision-making. The distributed model also reduces latency, avoids single points of failure, and enables localized responses tailored to mission-critical timing constraints. The Elastic Stack, including Kibana and LogStash, is used to implement the core Airspace-Manager Cybersecurity Function.

The data plane is responsible for continuously collecting telemetry and attestation evidence from UASs, as well as telemetry data from network resources and ground-based sensors, in support of the cybersecurity functions implemented by the service. Relevant UAS cyber telemetry is collected using a computationally-lightweight software module on board the UAS, which is paired with the Airspace-Manager Cybersecurity Function for data transmission/ingest. In our current implementation, this telemetry collection function is implemented on a companion processor on board the drone (e.g., Radxa Zero 3W), although it potentially also could use the drone's native Guidance Navigation & Control (GNC) processor. Physical performance data of the drone (e.g., geolocation, speed) can also be ingested, to support behavioral analysis for identity management and event monitoring. The system also allows hardware-backed cryptographic attestation, provided that an on-board processor has an integrated trusted platform module (TPM). In this case, each drone periodically produces hardware-backed attestation data alongside operational telemetry, enabling continuous verification of both identity and behavior. In addition, telemetry from network resources (e.g., network usage patterns of UASs) and from ground assets (e.g., from ground-based surveillance systems) can be ingested, for behavioral analysis. Communications between UASs and the airspace manager can be flexibly implemented in multiple modalities (cellular, satellite, WiFi for indoors) using the companion processor, This allows encryption of communications using e.g. mutual Transport Layer Security (MTLS) certificate exchange.

The architecture is structured for continuous trust assessment and adaptive response, which is necessary in dynamic, adversarial environments such as high-density UAS operations. We also stress that the architecture is customized and context-aware, in that attestation, event detection/management, and response use UAS behavioral data and are tailored to operational requirements.

Figure 2 also gives an overview of the workflow for the developed cybersecurity service. Firstly, the workflow sequence is initiated by an attestation between an asset (e.g., UAS, sensor) and the Airspace Manager Cybersecurity Function, which is undertaken periodically for any asset associated with the airspace volume.. Upon successful or

unsuccessful completion of the attestation, a multi-stage detect and decision pipeline is followed. The pipeline includes: 1) identity verification, 2) threat detection and behavioral monitoring/analysis (SIEM function), 3) context-based threat identification (SIEM function), 4) context-aware threat characterization, 5) policy implementation, and 6) security/policy adaptation. The remainder of the section is focused on detailing each workflow step, and then discussing innovations related to the solution..

B. Attestation

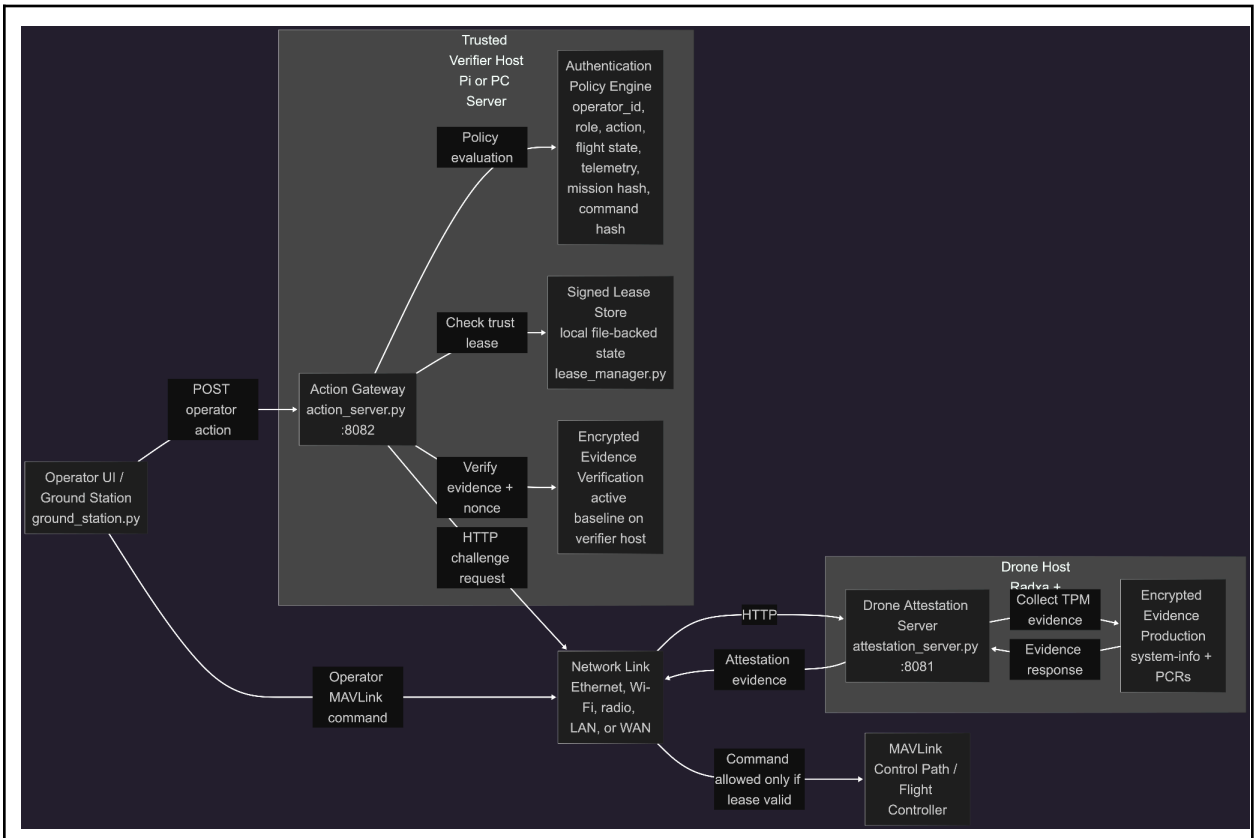

Figure 3: *Trust-gated UAS command architecture, showing how operator actions from the ground station are routed through a trusted verifier host before reaching the flight controller. The gateway checks identity, mission context, telemetry, command integrity, encrypted TPM-based drone evidence, and a signed trust lease before allowing MAVLink commands to continue to the drone control path.*

As an initial step, our cybersecurity service uses *attestation* – i.e. the provision of cryptographic evidence verifying authenticity – for engagement between UASs or other assets and the airspace-manager. The attestation step may be initiated by either the airspace manager or by the UAS (or other asset), with the manager-initiated attestation being the primary route. The airspace-manager-initiated attestation is diagrammed in Figure 3. Key steps in the attestation are the following. First, when the airspace manager indicates intent to communicate with an UAS, a verifier which is part of the Airspace Manager Cybersecurity Service is alerted. The verifier checks any policy regarding the need for attestation, with the default being that attestation is needed. The verifier also checks whether any leases indicating that attestation has been done within a sufficiently small time horizon (e.g. 5s) are open. If yes, then attestation is not needed, otherwise attestation is needed. In the case that attestation is needed, the verifier requests attestation to the UAS or other asset through the communication gateway. The request initiates a challenge to the UAS's attestation server, and the drone produces evidence that can be checked by the verifier. In our instantiation, the base evidence used for verification is a (hardware-backed) cryptographic signature from a Trusted Platform Module (TPM). Additionally, contextual data including UAS hardware/software and operational parameters can be used as evidence for attestation. The verifier return ALLOW or DENY, whereupon based on policy the communication request is (or is not) processed.

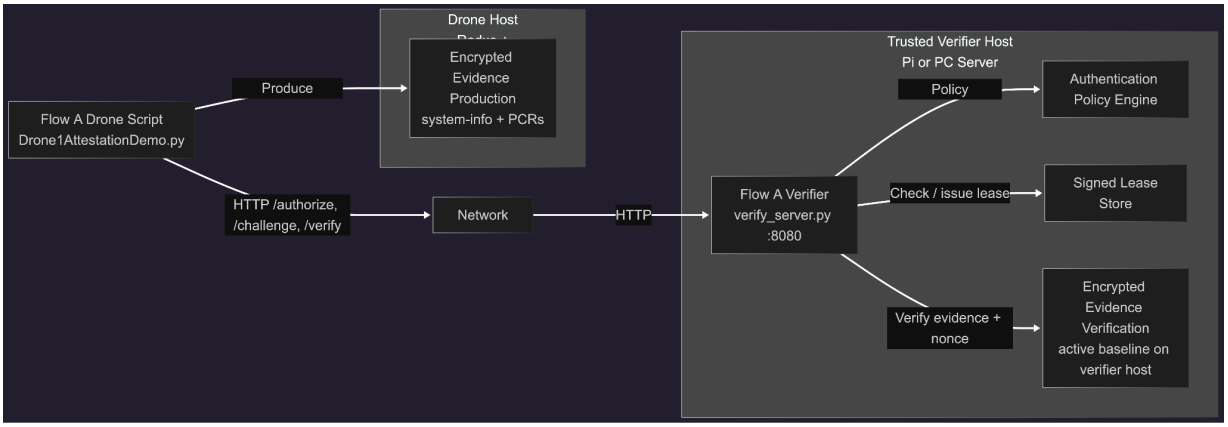

Figure 4: *TPM-based drone attestation workflow, showing how the drone produces encrypted system and PCR evidence, sends authorization and verification requests over HTTP, and relies on a trusted verifier host to validate the evidence against an active baseline. The verifier evaluates policy, checks or issues a signed lease, and uses nonce-based verification to ensure the drone's trust state is fresh before authorizing subsequent actions.*

The alternate UAS-initiated attestation is shown in Figure 4. The attestation is managed by a verifier which is part of the airspace manager's cybersecurity service. In broad terms, the UAS asks the verifier whether it is already authorized. If yes, engagement is initiated. If not, the verifier provides a nonce (a one-time-use token that is used to assure that the engagement is fresh and not a replay). Thereupon, the UAS produces local evidence that can be used for attestation, and sends the evidence to the verifier. As in the airspace-manager-initiated attestation, evidence includes a cryptographic key (associated with asymmetric or public-key encryption), which is used as a digital signature. In our setup, a TPM is used to store and produce the key. Additional contextual evidence including hardware and firmware metrics and UAS flight data, may also be provided. The verifier then checks the evidence and context, returns ALLOW or DENY, and (for ALLOW) issues a lease during which attestation need not be repeated.

C. Detection and Decision Pipeline:

The lower portion of Figure 2 illustrates the detection and decision pipeline, which transforms telemetry and TPM-based attestation evidence into actionable security decisions within the Airspace Manager Cybersecurity Function. This pipeline operates continuously, with updates on the order of 1–3 seconds, and integrates inputs from both the data plane (UAS telemetry and attestation evidence) and the control plane (mission context, geofencing constraints, and trusted identity baselines). In the current implementation, the pipeline is realized through the integration of a TPM-based verifier, a SIEM backend (Elastic Stack), and a rule-based policy engine. Future extensions will incorporate automated classification and adaptive policy refinement.

1. Identity Verification: The pipeline begins with identity verification using TPM-based remote attestation. Each drone periodically provides attestation evidence, including cryptographic identity and platform state measurements. The verifier evaluates this evidence using a challenge–response mechanism with nonce validation and compares it against approved baselines stored in the Central Context/Policy Database. Mission context, including geofencing constraints and assigned operational roles, is incorporated into the verification process. In the current system, this results in classification of each drone as trusted or untrusted, along with issuance of a short-lived trust lease when verification succeeds. This establishes a dynamic trust state rather than relying on static authentication.

2. Event Detection and Behavioral Monitoring (SIEM Rules): Following identity verification, telemetry is ingested into the SIEM backend for behavioral monitoring. Data sources include MAVLink command streams, network-level observations, and attestation outcomes. In this context, an "event" refers to any telemetry, communication, or system-level observation of concern associated with a UAS, including network activity, flight behavior, or system state changes. Logstash pipelines normalize and forward this

data to Elasticsearch, where it is indexed and queried in near real time.

Detection is performed using rule-based SIEM logic that combines multiple analysis mechanisms. These include text-based search and structured querying of logs using Elasticsearch and Kibana, as well as signature-based and pattern-based detection of anomalies in spatiotemporal data such as flight trajectories, network activity, and surveillance data. Using these capabilities, the system identifies anomalies such as communication irregularities, mission deviations, and geofence violations. Detection is context-aware, as rules are evaluated relative to mission/operations parameters and expected drone behavior rather than fixed thresholds. Detection alerts generated at this stage trigger downstream classification and response processes.

3. Event-Cause Classification. Detected anomalies are further analyzed to determine their likely cause. In the current implementation, this classification is performed using rule-based heuristics derived from observed telemetry patterns. For example, unexpected trajectory deviations combined with GPS inconsistencies may indicate spoofing, while repeated malformed command sequences may suggest command injection. Additional conditions such as heartbeat loss, abnormal communication latency, or repeated connection attempts from unknown sources are used to infer potential causes including jamming or denial-of-service activity.

4. Threat Characterization: The system then characterizes the threat in an operational context by combining identity verification results with detected anomalies. As shown in Figure 2, this stage distinguishes between (i) trusted drones under attack and (ii) malicious or non-compliant drones. A trusted drone exhibiting anomalous behavior is treated as a compromised asset requiring mitigation, whereas an unverified or inconsistent entity is treated as a potential rogue drone. This distinction is critical, as it determines whether the system prioritizes mission continuity or enforcement actions.

5. Response: Selection via the Policy Engine: The policy engine determines appropriate responses by integrating mission rules, geofencing constraints, trust levels, and threat classifications. Policy data is retrieved from the Central Context/Policy Database and applied locally within each Airspace Manager. In the current implementation, response selection is rule-based and designed to ensure that safety-critical constraints are preserved. For example, responses are selected to avoid destabilizing flight behavior while still enforcing cybersecurity policies. Future implementations will incorporate adaptive policy selection based on historical system performance and threat patterns.

6a. Response: Trusted Drone: For drones that are verified but exhibiting anomalous behavior, the system applies mitigation strategies aimed at preserving mission continuity. These include operator notification, enforced re-attestation, fail-safe modes, and communication or mission reconfiguration. In the current testbed, operator alerts and verifier-triggered re-attestation are implemented, while automated mission reconfiguration is planned for future work.

6b. Response: Non-Compliant or Malicious Drone: For untrusted or non-compliant drones, stronger enforcement actions are applied. These include command rejection, access revocation, and network segmentation to isolate the entity from the operational network. Additional measures such as monitoring escalation and policy enforcement triggers are supported within the architecture. In the current implementation, command gating via the verifier and alert generation are functional, while full automated network segmentation is under development.

7. Closed-Loop Adaptive Security: The pipeline operates in a closed-loop manner, where detection outcomes and response actions are fed back into the system to update future decisions. SIEM events, attestation results, and response outcomes are stored in the telemetry database and used to update policy state, trust evaluations, and detection rules. For example, repeated anomalies may reduce trust lease durations or trigger stricter verification requirements. These updates are shared with the Central Context/Policy Database, enabling consistency across airspace regions while allowing localized decision-making. Although current updates are rule-based, the architecture is designed to support adaptive learning mechanisms that refine detection and response strategies over time.

D. Context-Aware SIEM Integration:
A defining feature of the architecture is the tight integration between SIEM analytics and mission context. Traditional SIEM systems operate on logs in isolation. In contrast, the proposed system enriches telemetry with: 1) hardware-backed identity and attestation results; 2) UAS behavioral signatures, including network and flight telemetry; 3) operational assignments and geofencing constraints; and 4) historical behavioral baselines. This enriched telemetry enables context-aware correlation, allowing the system to: 1) determine whether an anomaly has occurred using multiple sources of evidence; 2) assess whether the anomaly is operationally significant; and 3) select an appropriate response consistent with mission requirements.

To illustrate this capability, consider a drone assigned to a corridor mapping mission within a defined geofence. During flight, the SIEM backend observes a trajectory deviation combined with inconsistent GPS readings, while the verifier indicates that the drone remains attested and within a valid trust lease. In a traditional SIEM, this deviation would likely trigger a generic anomaly alert. In the proposed system, however, the anomaly is evaluated in context: the mission requires strict adherence to a predefined path, and the deviation exceeds allowable tolerance while occurring in a region associated with elevated GPS interference risk.

The SIEM correlates the trajectory anomaly, GPS inconsistency, and maintained attestation integrity, and classifies the event as a likely GPS spoofing attempt on a trusted drone rather than a navigation error or an unverified entity. Based on this classification, the policy engine selects a response that preserves mission safety while mitigating risk. Specifically, the system triggers operator notification, enforces re-attestation to confirm system integrity, and constrains the drone to a fail-safe mode such as hover or return-to-home while maintaining communication links.

If the same trajectory deviation were observed under different conditions, the system would produce a different classification. For example, in a mission with flexible routing, such as exploratory inspection, the deviation may be interpreted as acceptable mission variation. Alternatively, if the deviation were associated with a drone lacking valid attestation, the system may classify the entity as non-compliant or potentially malicious. In these cases, the response would differ accordingly, ranging from continued operation to access revocation or communication restriction. This example demonstrates how the integration of SIEM analytics with mission context enables differentiated, operation-aware decision-making, rather than static anomaly response.

E. Hybrid Data Architecture:
The proposed system adopts a hybrid data architecture, which separates authoritative operational data from high-volume telemetry and analytics data while allowing controlled interaction between the two. In general, a hybrid data architecture refers to a design in which different classes of data are stored, processed, and accessed using distinct systems optimized for their specific roles, rather than relying on a single unified database. This approach is commonly used in cyber-physical and real-time systems where both low-latency decision-making and large-scale data ingestion and analysis are required. By decoupling these functions, the architecture improves scalability, system performance, and reliability, while also supporting auditability and regulatory compliance.

In the context of UAS operations, this separation is particularly important because operational decisions such as trust evaluation and command authorization must be executed with minimal latency, whereas telemetry data such as network activity, flight logs, and attestation records may be generated at high volume and require more computationally intensive analysis. The hybrid model ensures that real-time decision-making is not delayed or disrupted by large-scale data processing tasks.

The architecture is structured into three primary data components:

1. ***Global Control-Plane Database:*** A centralized control-plane database, implemented using ScyllaDB, maintains the authoritative system state. This includes UAS identity records (e.g., cryptographic signatures and TPM bindings), mission assignments, geofencing constraints, operational baselines, and policy rules. The database is designed for low-latency access and high availability, enabling consistent policy enforcement across multiple airspace regions. It serves as the source of truth for identity verification, trust evaluation, and response selection within the detection and decision pipeline.

2. ***Local Caches:*** Each Airspace Manager maintains a local cache of relevant control-plane data to support

real-time decision-making at the edge. These caches store mission-critical information such as active drone identities, trust states, and policy subsets required for the current airspace region. By avoiding repeated queries to the centralized database, local caches reduce latency and enable rapid execution of verification and response actions. Updates to trust states and policy changes are periodically synchronized with the global control-plane database, ensuring consistency while preserving responsiveness.

3. ***SIEM and Telemetry Store:*** A dedicated telemetry and analytics layer, implemented using Elasticsearch, is used to store high-volume event data. This includes attestation outcomes, MAVLink telemetry, network observations, and SIEM-generated alerts. Unlike the control-plane database, this store is optimized for indexing, searching, and correlating large volumes of time-series data. It supports real-time anomaly detection as well as long-term storage for forensic analysis, system auditing, and adaptive security improvements. The SIEM backend operates directly on this data, generating alerts that are fed back into the decision pipeline.

In its current implementation, the hybrid architecture operates with clear functional separation and limited automated synchronization. Future work will enhance this integration by enabling more dynamic data exchange between layers, including automated policy updates based on SIEM analytics and distributed consistency mechanisms across airspace regions. Even in its current form, the hybrid data architecture provides a scalable and resilient foundation for supporting real-time, context-aware cybersecurity in complex UAS environments.

IV. Instantiation and Testing

The cybersecurity solution has been instantiated in a laboratory testbed at the Global Cyber Research Institute (GCRI) at Texas A&M University, and initial tests of cybersecurity functions focusing on attestation have been pursued. In this section, the laboratory testbed, instantiation of the security solution, and initial testing outcomes are described.

A. Laboratory Testbed and Cybersecurity Solution Instantiation

A testbed has been constructed for assessing the impacts of cyber threats on complex UAS operations. The testbed allows multi-UAS flights within a 10 ft x 10 ft x 10 ft drone cage (Figure 5). In the long term, the testbed is intended to allow visual-line-of-sight and beyond visual-line-of-sight operations, with either a flight operator or a separate flight coordinator being responsible for airspace management (collision avoidance, etc). For this study, manual control of a single UAS through a Wi-Fi-based local network was implemented. The UAS used in the testbed is a custom 5-inch quadrotor built on a QAV-S 2 frame and equipped with a TBS Lucid H7 V2 flight controller (STM32H743 processor) running ArduCopter V4.6.1 as its guidance, navigation, and control (GNC) firmware. The flight operator is provided with a RadioMaster TX16S transmitter operating in USB joystick mode, which feeds into a Raspberry Pi 4B that hosts the Airspace Manager's UTM functions and represents the ground-side compute node (see Figure 5). The Raspberry Pi 4B communicates with the UAS through a local Wi-Fi network within the GCRI laboratory. Specifically, it communicates with a companion processor on board the UAS, selected as a Radxa Zero 3W because of its favorable weight, form factor, and 40-pin GPIO support for an integrated hardware root of trust. The companion processor relays authorized MAVLink commands to the TBS Lucid H7 flight controller over UART, where the GNC firmware translates them into low-level motor and attitude control.

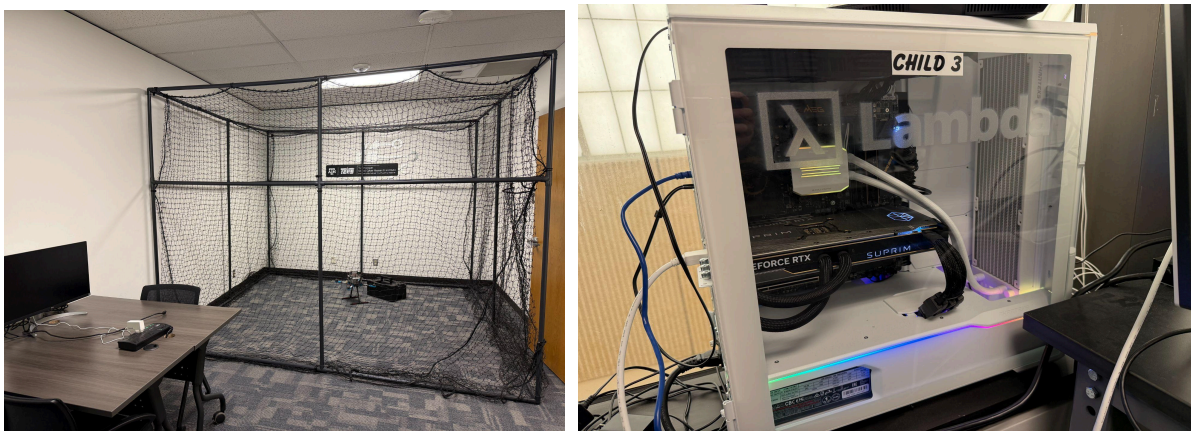

Figure 5: *Cybersecurity service evaluation testbed, including an indoor drone cage for controlled multi-UAS operations and a Lambda Vector One compute node for implementing UTM functions and emulating cyber threats. The compute node is equipped with an AMD Ryzen 9 7950X CPU, NVIDIA RTX 4090 GPU, 64 GB memory, and Ubuntu 22.04 with Lambda Stack for TensorFlow, PyTorch, CUDA, cuDNN, and related software dependencies.*

The developed cybersecurity solution has been instantiated in part in the laboratory testbed, with the current implementation focused on TPM-backed authentication, verifier-based authorization, and SIEM data ingestion. The deployed system follows the trust-gated architecture described earlier in the paper: drone commands are not treated as automatically valid simply because they originate from the ground station. Instead, command authority is mediated through a verifier host that checks device identity, attestation evidence, policy state, and recent trust history before allowing the action to proceed.

The hardware root of trust in the current implementation is used through the LetsTrust TPM connected to the UAS-side companion computing platform which is the Radxa 3W Zero. The TPM acts as a protected cryptographic component that stores or protects identity and produces hardware-backed evidence about the state of the device. In the implemented workflow, the drone-side module collects TPM-based evidence, including platform configuration information such as Platform Configuration Register (PCR)-derived measurements, and sends the evidence to the trusted verifier. The purpose of this evidence is to demonstrate that the UAS-side computing environment is in an expected and approved state before it is allowed to conduct a sequence of actions on the drone.

The verifier is hosted on the ground-side computer server associated with the airspace-manager cybersecurity function. Its role is to evaluate whether the UAS should be treated as trusted for the requested operation. The verifier issues or checks a fresh challenge, validates the returned evidence, compares it against an approved baseline, and then returns an authorization decision. This challenge-response structure is important because it prevents stale evidence from being reused in a replay attack. When verification succeeds, the verifier can issue a short-lived signed trust lease. This lease allows subsequent commands to proceed without requiring a full attestation exchange before every individual action, while still limiting the time window in which trust remains valid. We implement this design for UAS operations because excessive reauthentication delays could interfere with time-sensitive control, while permanent trust would be unsafe in a changing cyber environment.

The cryptographic evidence production and verification logic is implemented using a Beyond Identity-based crypto module [13], which provides the software mechanism for producing structured attestation evidence and validating on the verifier side. In the current testbed, this module is used to bind the drone's identity and measured platform state to cryptographic proof. The drone-side component produces encrypted or signed evidence from the TPM-backed state, while the verifier-side component checks that evidence against the active reference baseline before allowing command authority. This provides a practical implementation of remote attestation within the UAS testbed rather

than relying only on conventional network login or static credentials.

A preliminary SIEM backend has been integrated into the Airspace Manager Cybersecurity Function on the Raspberry Pi 4B ground server, in support of context-aware event monitoring. This SIEM backend provides a centralized mechanism for ingesting, correlating, and visualizing security-relevant events across the UAS system, and serves as the implementation of the event detection and behavioral monitoring stages described in the detection and decision pipeline. While not yet a production-scale deployment, the current implementation demonstrates the feasibility of tightly coupling telemetry analysis with attestation and mission logic.

The SIEM backend is implemented using the Elastic Stack (Elasticsearch, Logstash, and Kibana). Logstash serves as the ingestion layer, receiving structured JSON telemetry over a TCP interface from multiple system components, including the verifier, drone-side modules, and network monitoring processes. Incoming events are parsed and normalized before being indexed in Elasticsearch as time-series records, enabling both real-time querying and retrospective analysis.

Consistent with the detection and decision pipeline, three primary classes of telemetry are ingested to support identity verification, event detection, and threat characterization. First, attestation and identity events are generated by the verifier and include challenge issuance, nonce validation, attestation outcomes (ALLOW/DENY), lease issuance, and associated failure reasons. As shown in Figure 6, structured fields such as decision and reason are indexed, enabling tracking of trust state transitions over time. Second, flight and command telemetry derived from MAVLink messages provides visibility into command execution and drone behavior. Although currently limited in scope, this data enables correlation between issued commands and attestation state, forming the basis for detecting anomalous command patterns. Third, network-level observations, including source IP addresses and communication endpoints, support identity-to-network binding. As illustrated in Figure 7, SIEM rules associate observed network activity with known drone identities, enabling detection of unauthorized or unexpected communication sources.

Within Elasticsearch, these heterogeneous data streams are unified into a single searchable index, allowing cross-domain correlation between identity, behavior, and network activity. Kibana dashboards provide operator-facing visualization, including alert summaries, rule triggers, and event timelines. In addition to visualization, alerting rules are configured such that when a previously unseen network source is detected, a “new object” or “new entity” alert is generated, corresponding to a device entering the monitored airspace. This alert persists the associated source IP address and metadata within the SIEM data store, effectively maintaining a record in the ScyllaDB of newly observed entities for subsequent correlation with identity and attestation events. For example, Figure 6 illustrates how attestation failures are surfaced as structured SIEM events and Figure 7 presents a rule-based alert view in which repeated connections from specific IP addresses are aggregated, flagged, and stored.

Detection logic is implemented using Kibana alerting rules and query-based filters. Current rules include: (1) attestation failure detection, which triggers alerts when a drone repeatedly fails verification or produces invalid evidence; (2) identity–IP mismatch detection, which flags inconsistencies between observed network sources and expected drone identities; and (3) unexpected activity detection, which identifies deviations in communication frequency or command issuance relative to baseline behavior. Although these rules are heuristic and manually defined, they represent an initial step toward aviation-specific anomaly detection tailored to UAS operations.

Importantly, SIEM-generated alerts are integrated into the broader cybersecurity workflow rather than operating as passive indicators. Detected events are fed back into the Airspace Manager Cybersecurity Function, where they inform policy decisions such as forced re-attestation, lease revocation, or operator notification. In this way, the SIEM backend directly supports the transition from event detection to policy-driven response, enabling the closed-loop adaptive security behavior described earlier in the architecture.

At its current stage, the SIEM backend operates as a semi-integrated monitoring layer with limited automation in

response execution. However, the architecture is designed to support tighter coupling in future work, enabling SIEM-derived insights to directly trigger mitigation actions in real time. Even in its preliminary form, the system demonstrates the viability of combining hardware-backed identity through TPM-based attestation with centralized log analytics to achieve context-aware, mission-relevant intrusion detection in UAS environments.

B. Tests Conducted and Results

Initial testing in the laboratory testbed focused on validating the end-to-end command and monitoring pipeline that the cybersecurity service is designed to mediate. These tests were conducted to verify that the underlying communication, control, and telemetry infrastructure operates correctly prior to full integration of trust-gated security mechanisms.

1. End-to-End Command Pipeline Validation:
The test connected the RadioMaster TX16S transmitter to the Raspberry Pi 4B ground server in USB joystick mode and verified that operator stick inputs were correctly read on the ground side. The Raspberry Pi 4B then established an IP-based MAVLink link over the local Wi-Fi network to the Radxa Zero 3W companion processor on board the UAS. On the drone side, the companion processor forwarded the received MAVLink commands to the TBS Lucid H7 flight controller over UART, where ArduCopter V4.6.1 translated them into vehicle control actions. Operator stick movements at the TX16S produced corresponding responses at the flight controller, confirming that the full chain from the transmitter, through the ground server and the IP link, through the companion processor, and into the GNC firmware was functioning as intended.

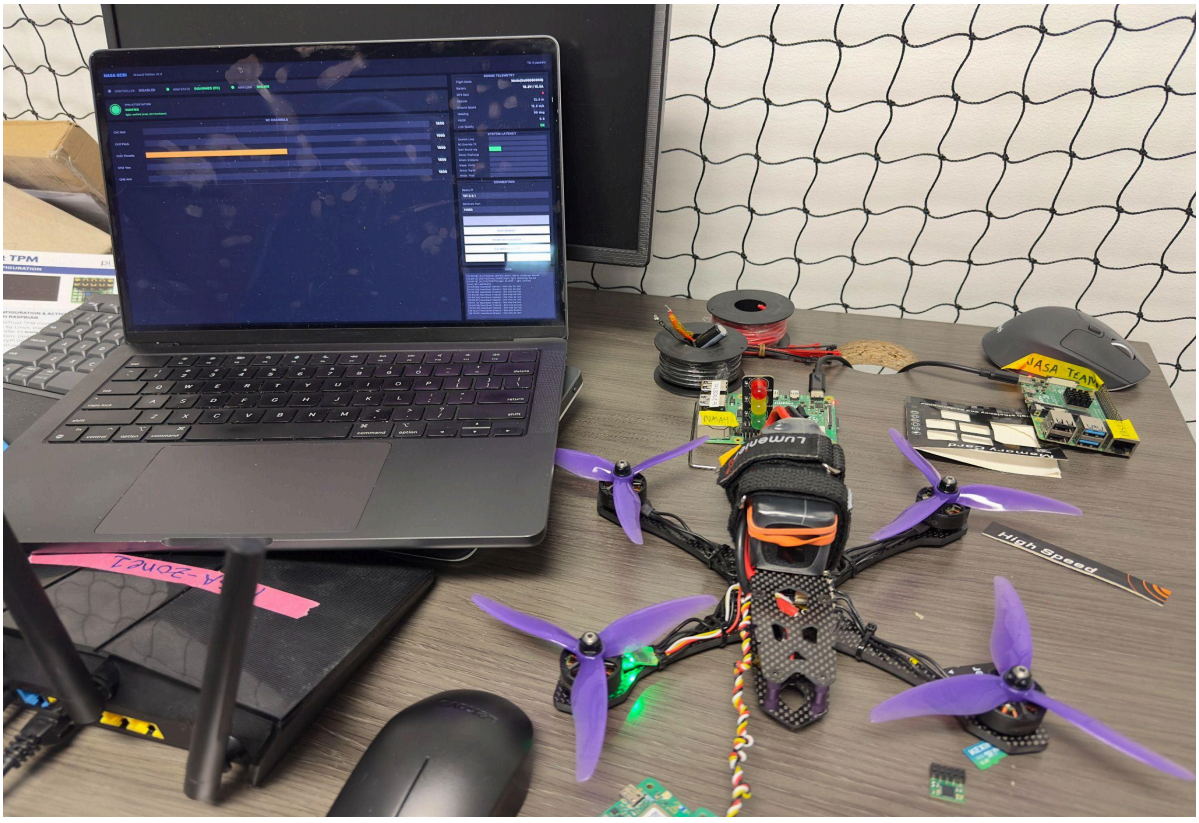

Figure 6: End-to-end command pipeline test setup in the GCRI laboratory.

2. Airspace-Manager- and UAS- Initiated Attestation Check

Testing also exercised the two attestation flows described in Section III.B, in standalone form prior to their integration into the live MAVLink command path. Both the airspace-manager-initiated flow (Figure 3) and the UAS-initiated flow (Figure 4) were validated end-to-end across the testbed hardware. In both cases, evidence production was performed on the drone-side hosted on a Raspberry Pi 4B using the LetsTrust TPM as the hardware root of trust, while validation was performed by the verifier hosted on a laptop ground server. The Beyond Identity-based crypto module provided the underlying mechanism for producing signed evidence on the drone side and validating it against the active baseline on the verifier side.

For the UAS-initiated flow, the drone-side attestation client issued an authorization request to the verifier. When no valid lease was present for the requesting drone, the verifier responded with a fresh nonce. The drone-side module then collected TPM evidence, i.e. PCR-derived platform measurements bound to the nonce, and returned the structured evidence to the verifier via the /verify endpoint. The verifier validated the cryptographic signature, compared the platform measurements against the approved baseline, and returned an ALLOW or DENY decision. In the ALLOW case, the verifier additionally issued a short-lived signed lease that was persisted in the local lease store. When the same drone subsequently issued an /authorize request within the lease window, the verifier returned the existing lease without requiring repeated TPM evidence production, confirming that the lease-based optimization behaves as designed.

For the airspace-manager-initiated flow, the action gateway was exercised as the entry point for operator commands. Before forwarding any action toward the drone, the gateway consulted the lease store and, in the absence of a valid lease, issued an HTTP challenge to the drone-side attestation server (attestation_server.py on port 8081). The drone returned fresh TPM-backed evidence, which the verifier validated through the same baseline check used in the UAS-initiated path. On a successful evaluation, the gateway issued a lease and permitted the operator action to proceed; on a failed evaluation, the gateway blocked the action at the trust-gate.

To verify rejection behavior, negative test cases were exercised. These included presenting evidence whose PCR values did not match the approved baseline (which would emulate a drone-side software state change) and submitting evidence after lease expiry such that the bound nonce was no longer fresh. In both cases, the verifier returned a DENY decision. These results validate that both attestation flows operate as specified.

3. Attestation Event Logging and Correlation:

Testing also confirmed the correct ingestion and structuring of TPM-based attestation events within the SIEM backend. The attestation workflow described in Figure 4 is directly reflected in the SIEM as structured event data in real time. Specifically, verifier outputs, including challenge issuance, evidence validation, and final authorization decisions (ALLOW or DENY) along with associated failure reasons, are transmitted through the ingestion pipeline and indexed in Elasticsearch.

As illustrated in Figure 6, these events provide a time-resolved view of the attestation process from the perspective of the monitoring system. Each step in the attestation exchange, including nonce validation and trust lease evaluation, is captured as a structured SIEM event, enabling tracking of trust state transitions over time. This establishes a direct linkage between the attestation mechanism and the behavioral monitoring layer, allowing identity verification outcomes to be correlated with observed system and network behavior.

This result demonstrates that the system not only performs attestation at the control level, but also externalizes attestation outcomes into the SIEM layer for continuous monitoring, anomaly correlation, and downstream decision-making within the detection and decision pipeline.

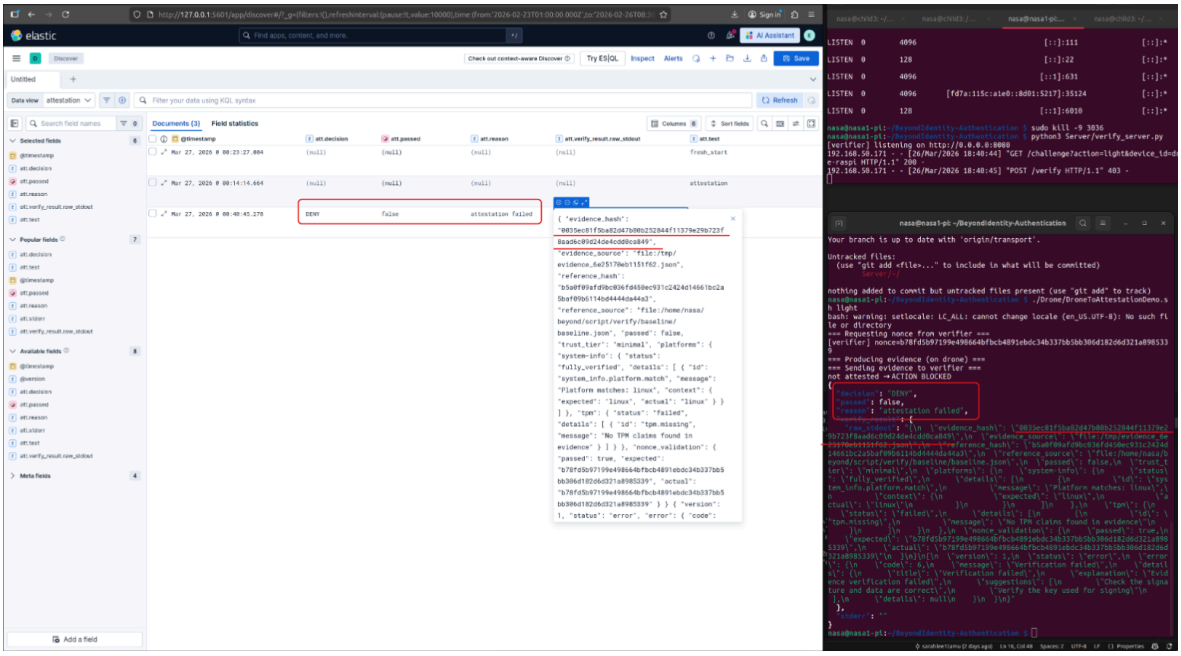

Figure 7: *SIEM visualization of TPM-based attestation events corresponding to the workflow shown in Figure 4, illustrating structured logging of verifier decisions (ALLOW/DENY), nonce validation, and associated failure reasons. These events enable tracking of trust state transitions and correlation between identity verification outcomes and system behavior.*

4. SIEM Telemetry Ingestion and Visualization:
A second set of tests validated the ingestion and visualization of telemetry within the SIEM backend. Attestation events, MAVLink-derived telemetry, and network observations were successfully transmitted to the Logstash ingestion pipeline and indexed within Elasticsearch. Kibana dashboards correctly displayed event timelines, alert summaries, and identity-related metadata. As shown in Figure 7, rule-based alerts successfully aggregated repeated connections from specific source IP addresses, demonstrating the ability to detect and visualize anomalous communication patterns.

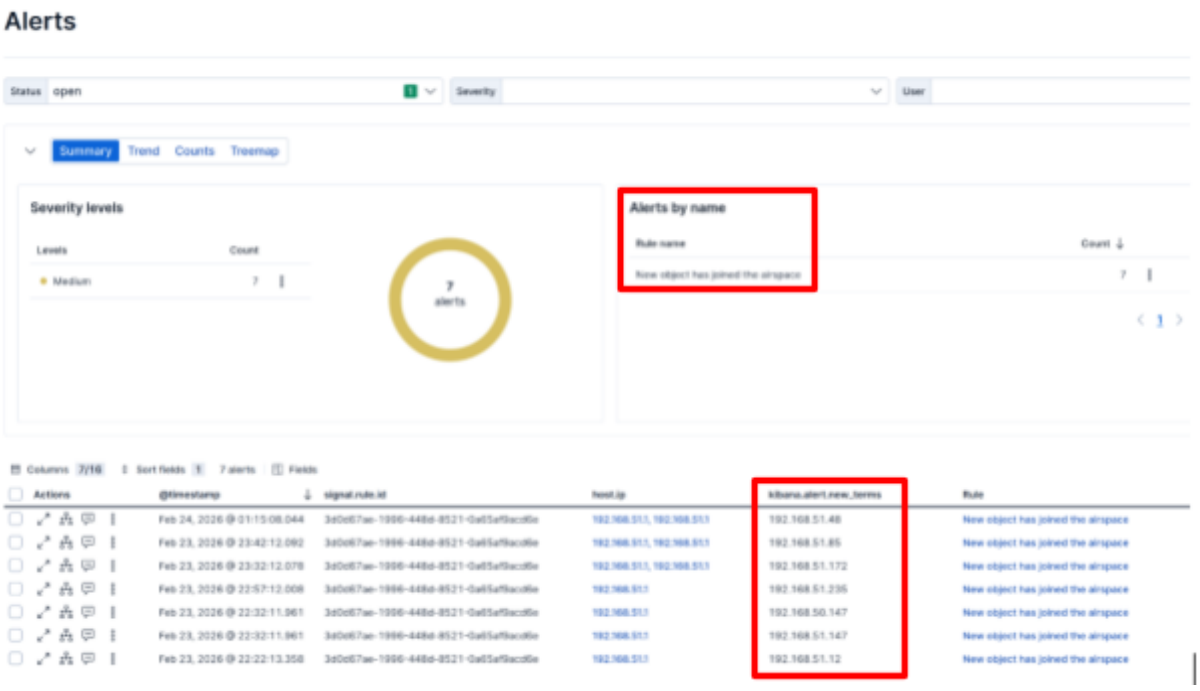

Figure 8: *SIEM rule-based alert view showing correlation of network source IP addresses with observed UAS activity. The dashboard aggregates repeated connections and flags identity–network mismatches, enabling detection of unauthorized or unexpected communication sources within the monitored airspace.*

These results collectively validate that the communication pipeline, telemetry ingestion mechanisms, and SIEM-based monitoring infrastructure operate as intended. The successful integration of command execution and event monitoring establishes a functional foundation for the trust-gated architecture described in Section IV.A. Ongoing work focuses on integrating the verifier and policy enforcement mechanisms into the live control path, enabling real-time attestation-driven command authorization and automated response to detected threats.

C. Discussion

The direct motivation for developing the cybersecurity service described here is to help aviation stakeholders meet the cybersecurity requirements of the proposed FAA rule for normalized BVLOS operations. The requirements of the FAA rule dictate that stakeholders must ensure appropriate cybersecurity protocols, and also have working event or intrusion management systems. While there is a deluge of commercial tools for these functions, UAS operations in the airspace entail a number of custom features and challenges, which make the application of these standard tools challenging. Our solution aims to customize cybersecurity functions for complex UAS operations in the airspace, and specifically for UTM. Thus, we believe that the solution is a timely enabling technology for the normalization of UAS operations.

Contributions and Acknowledgments

The first three authors contributed equally to this work. SL was primarily responsible for developing the detect & decision pipeline including SIEM capability. MA led the development of the attestation function as a whole, with KL developing the UAS-initiated workflow. OM led the integration of the cybersecurity function within the UAS testbed. JK advised the first four authors in architecting the cybersecurity solution. SR envisioned the context-aware cybersecurity approach as a whole, and helped to scope the solution for practical application to future UTM applications. SL, MA, and SR were primarily responsible for drafting the manuscript. The authors also acknowledge collaborations with J. Dixson and B. Ashby at Beyond Identity Corporation, and N. Truong at Texas A&M. The authors also gratefully acknowledge support provided by the National Aeronautics and Space Administration.

References

[1] Sampigethaya, Krishna, Parimal Kopardekar, and Jerry Davis. "Cyber security of unmanned aircraft system traffic management (UTM)." In *2018 Integrated Communications, Navigation, Surveillance Conference (ICNS)*, pp. 1C1-1. IEEE, 2018.

[2] Pascarella, Domenico, Gabriella Gigante, Angela Vozella, Pierre Bieber, Thomas Dubot, Albert Remiro Bellostas, and Jaime Cabezas Carrasco. "A Preliminary Concept for a Resilience Service to Manage Drone Cyber-Physical Attacks." In *2024 IEEE International Workshop on Technologies for Defense and Security (TechDefense)*, pp. 351- 356. IEEE, 2024.

[3] Lewis, Terrence, Steve W. Garcia, and Ainaz Estiri. "Cyber Resiliency and the Implementation of a Host-Based Intrusion Detection System in an Urban Air Mobility Environment." In *AIAA AVIATION FORUM AND ASCEND 2024*, p. 4638. 2024.

[4] Abdulrazak, Charles. "Cybersecurity Threat Analysis And Attack Simulations For Unmanned Aerial Vehicle Networks." *arXiv preprint arXiv:2404.16842* (2024).

[5] Roy, Sandip, Vishwam Raval, Kevin Lei, Oscar Leon, Jaewon Kim, Chenyan Zhu, and Oluwafemi Ajeigbe. "Testbed for Cybersecurity Assessment of UAS Traffic Control." In *AIAA AVIATION FORUM AND ASCEND 2025*, p. 3311. 2025.

[6] Lykou, Georgia, George Iakovakis, and Dimitris Gritzalis. "Aviation cybersecurity and cyber-resilience: Assessing risk in air traffic management." In *Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies*, pp. 245-260. Cham: Springer International Publishing, 2019.

[7] Johnson, Chris W. "Cyber security and the future of safety-critical air traffic management: identifying the challenges under NextGen and SESAR." In *10th IET System Safety and Cyber-Security Conference 2015*, pp. 1-6. IET, 2015.

[8] Hamza, Muhammad Ameer, Mujahid Mohsin, Mohsin Khalil, and Syed M. Kazam Abbas Kazmi. "Mavlink protocol: A survey of security threats and countermeasures." In *2024 4th International Conference on Digital Futures and Transformative Technologies (ICoDT2)*, pp. 1-8. IEEE, 2024.

[9] Federal Aviation Administration. *Normalizing Unmanned Aircraft Systems Beyond Visual Line of Sight Operations*. ***Federal Register*** [Document 2025-14992], August 7, 2025.

[10] Thahsin, A., Ananthapadmanabhan, A., Pathak, S., Maity, A., and Kasbekar, G. S., "Enhancing MAVLink Security: Implementation and Performance Evaluation of Encryption on a Drone Testbed," ***2025 39th International Conference on Information Networking (ICOIN)***, Jan. 2025.

[11] Yoo, D., Tak, T., Kim, T., and Han, S., "Preliminary Study on Cyberattack Impacts on Drone Flight Control," presented at the Korean Nuclear Society Autumn Meeting, Changwon, Korea, Oct. 30–31, 2025.

[12] Krishna, CG Leela, and Robin R. Murphy. "A review on cybersecurity vulnerabilities for unmanned aerial vehicles." In *2017 IEEE international symposium on safety, security and rescue robotics (SSRR)*, pp. 194-199. IEEE, 2017.

[13] Beyond Identity, "Beyond Identity," Available: https://www.beyondidentity.com.