Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

A Secure Boot and Tamper-Resistant Firmware Framework for UAV Systems

Archana Kotakar
Department of Computer Engineering
JSPM's JSCOE, Pune

Vishal Gajanan Zalake
Department of Computer Engineering
JSPM's JSCOE, Pune

Vaishnavi Vijay Saraf
Department of Computer Engineering
JSPM's JSCOE, Pune

RadheyParikshit Bildikar
Department of Computer Engineering
JSPM's JSCOE, Pune

Smitesh Vivek Shinde
Department of Computer Engineering
JSPM's JSCOE, Pune

Abstract - Unmanned Aerial Vehicles (UAVs) are increasingly being utilized in mission-critical applications such as defense, surveillance, and disaster response, where reliability and security are essential. However, the growing dependence on UAV technology has also increased the risk of cyber threats, particularly those targeting firmware, which can be manipulated to gain unauthorized control or disrupt system operations. This paper proposes a secure UAV framework that enhances firmware integrity and safeguards against unauthorized parameter modifications through the integration of secure boot and cryptographic authentication techniques. The framework employs SHA-256 hashing in combination with asymmetric cryptography to validate firmware authenticity before execution, ensuring that only trusted firmware is allowed to run on the system. In addition, a runtime authentication mechanism based on a nonce-driven challenge-response protocol and digital signatures is introduced to restrict unauthorized access from Ground Control Stations (GCS). The proposed approach is implemented using the ArduPilot platform, Pixhawk flight controller, and MAVLink communication protocol. Designed to be lightweight and scalable, the framework is well suited for resource-constrained embedded UAV environments. Experimental observations indicate that the system effectively prevents the execution of unauthorized firmware while enforcing secure access control for critical parameter modifications.

Keywords - cyberattacks, defense, UAV firmware, SHA-256, asymmetric cyptography, GCS, Pixhawk, ArduPilot, MAVLink

I. INTRODUCTION

Unmanned Aerial Vehicles (UAVs), commonly referred to as drones, have transformed the way numerous industries operate. Their applications now extend across defense operations, disaster response, agricultural monitoring, logistics, environmental surveillance, and many other mission-critical domains. The growing reliance on UAVs is primarily driven by their ability to perform complex tasks with improved efficiency, accuracy, and reduced human intervention. These systems function either autonomously or semi-autonomously through embedded controllers and firmware responsible for navigation, communication, flight stability, and payload management. Despite these advantages, the widespread adoption of UAV technology has introduced significant cybersecurity concerns. The firmware embedded within a UAV acts as the foundation of its operation and is therefore an attractive target for malicious attacks. Unauthorized modifications, firmware tampering, and code injection can compromise the integrity of the system, resulting in unauthorized access, loss of control, privacy violations, or even physical harm during safety-critical missions. Such vulnerabilities highlight the importance of ensuring that only authentic and trusted firmware is permitted to execute on UAV platforms.

The increasing use of drones in sensitive sectors has also created a growing demand for secure and resilient UAV systems. Government agencies, defense organizations, research institutions, and industrial operators are actively seeking drone technologies capable of resisting cyber threats while maintaining reliable performance. Applications involving surveillance, border security, disaster management, and critical infrastructure require UAVs that cannot be easily manipulated or hijacked by unauthorized entities. Consequently, firmware protection and access control mechanisms are emerging as essential requirements in the development of next-generation aerial systems. To address these challenges, this work proposes a secure UAV framework designed to enhance firmware integrity and prevent unauthorized access. The proposed solution incorporates a secure boot mechanism based on asymmetric cryptographic techniques. During the firmware generation process, the code is digitally signed using a private key. When the UAV is powered on, the flight controller verifies this signature using the corresponding public key stored within its memory. This verification process ensures that only authenticated and untampered firmware is executed on the hardware.

The proposed framework not only ensures firmware authenticity through secure boot validation but also incorporates a key-based authentication mechanism to protect critical flight parameters from unauthorized modifications. Ground Control Stations such as Mission Planner enable users to adjust configuration settings for operational purposes; however, compromised

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

communication channels can expose these features to potential misuse. To address this concern, an additional authentication layer is integrated into the ArduPilot environment, allowing only verified users to make parameter changes. By combining cryptographic firmware verification with runtime access control, the system enhances the overall security and resilience of UAVs against cyberattacks and unauthorized operations. The framework is implemented using the ArduPilot ecosystem, with cryptographic modules developed in C++ and Python, and is deployed on a Pixhawk flight controller while utilizing Mission Planner for configuration, testing, and evaluation. This approach contributes to the development of trustworthy and cyber-secure UAV platforms capable of meeting the safety and reliability requirements of critical applications.

II. BASE PAPER OVERVIEW

The paper "Electronic Warfare Cyberattacks, Countermeasures, and Modern Defensive Strategies of UAV Avionics" by Aaron Yu, Iuliia Kolotylo, Hashim A. Hashim, and Abdelrahman E. E. Eltoukhy, published in IEEE Access (2025) with the DOI 10.1109/ACCESS.2025.3561068, provides a comprehensive overview of modern cyberattacks targeting UAV avionics systems. The authors emphasize that firmware-level vulnerabilities significantly expose UAVs to exploitation, making them susceptible to a range of advanced electronic warfare tactics. [1] The study categorizes cyberattacks into three main types: communication interception, firmware injection, and hardware manipulation. Each category represents a different layer of vulnerability within UAV systems, illustrating how attackers can compromise data transmission, alter embedded software, or directly manipulate physical components. [1] To address these vulnerabilities, the authors propose several defensive strategies, including the integration of cryptographic validation mechanisms, secure boot sequences, and intrusion detection systems. These countermeasures aim to enhance UAV resilience by ensuring that only authenticated and verified code can be executed, while also providing real-time monitoring against unauthorized access or tampering attempts. [1]

The paper "Understanding and Securing the Risks of Uncrewed Aerial Vehicle Services" by Ioannis Anagnostis, Panayiotis Kotzanikolaou, and Christos Douligeris, published in IEEE Access (2025) with the DOI 10.1109/ACCESS.2025.3549861, explores the risk factors associated with UAV systems operating in networked environments. The authors analyse how wireless communication links and cloud-based control systems increase the exposure of UAVs to various cyber vulnerabilities, making them potential targets for exploitation. [2] The study presents a risk quantification framework for UAV services, which classifies threats according to the confidentiality, integrity, and availability (CIA) triad. This framework enables systematic evaluation of potential security risks, helping identify areas where UAV systems are most susceptible to compromise. [2] Furthermore, the authors emphasize the importance of implementing both policy-based and technical safeguards to mitigate these risks. Key measures discussed include firmware verification and the use of encrypted communication channels to protect against unauthorized access and data manipulation. [2]

The paper "Sensor Deprivation Attacks for Stealthy UAV Manipulation" by Alessandro Erba, John H. Castellanos, Sahil Sihag, Saman Zonouz, and Nils Ole Tippenhauer, published on arXiv (2024) with the identifier 2410.11131v1, investigates stealthy cyberattacks that target UAV sensor systems without directly modifying the firmware. The authors demonstrate how manipulation of sensor input data can mislead UAV control logic, causing the system to perform unsafe or unintended behaviors while avoiding conventional detection mechanisms. [3] Although the study primarily examines sensor-level attack vectors, it highlights the crucial role of firmware-level integrity as a defense mechanism. The authors emphasize that if UAV firmware incorporates the ability to detect anomalies or verify the authenticity of input signals, it can effectively mitigate such stealthy manipulations before they result in operational compromise. [3] The insights from this research directly influenced our project's approach by motivating the extension of firmware integrity checks beyond boot-time validation. Building on these findings, our project proposes the future integration of real-time firmware-based anomaly detection modules to strengthen UAV resilience against sensor-level stealth attacks. [3]

The paper "A Security Review in the UAVNet Era: Threats, Countermeasures, and Gap Analysis" by A. Rugo, C. A. Ardagna, and N. E. Ioini, published in ACM Computing Surveys, Vol. 55, No. 1, January 2023, presents a comprehensive review of modern UAV networking (UAVNet) security challenges. The authors examine a wide range of vulnerabilities, including communication protocol weaknesses, firmware vulnerabilities, and network intrusion risks, outlining how these issues collectively undermine UAV system resilience. [4] The paper categorizes UAV security threats into three hierarchical levels — firmware-level, communication-level, and network-level — emphasizing that firmware integrity serves as the first and most critical layer of defense against cyberattacks. The authors discuss emerging trends such as the integration of cryptographic bootloaders, secure firmware update mechanisms, and remote attestation techniques designed to detect and prevent firmware tampering in UAV systems. [4] Additionally, the survey identifies a significant research gap in the development of lightweight firmware authentication methods that can be effectively implemented on resource-constrained flight controllers. Addressing this limitation is essential for achieving practical and scalable UAV security solutions. [4] This research is highly relevant to our project, as it provides a theoretical foundation for implementing asymmetric cryptography and key-based control

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

mechanisms to ensure firmware authenticity and maintain operational trustworthiness in UAV systems. [4]

III. PROPOSED SYSTEM

The proposed system is designed as a secure and modular UAV framework that integrates both hardware-level trust mechanisms and software-based cryptographic protections to ensure firmware integrity and controlled access. The architecture follows a layered approach, combining secure firmware deployment, authenticated communication, and real-time parameter protection.

At the hardware level, the system establishes a **root of trust** by securely storing cryptographic keys within protected memory regions such as secure flash or hardware-backed storage. This ensures that the public key used for verification cannot be altered by external entities. The hardware layer also supports authentication anchoring, enabling the system to enforce security policies even during flight operations. In case of any security violation, such as detection of tampered firmware, the system transitions into a failsafe mode to prevent unsafe UAV behavior.

The firmware layer is built on the ArduPilot core, where the firmware image is cryptographically signed before deployment. During execution, the system performs hash calculations using algorithms such as SHA-256 to verify firmware integrity. A policy enforcement mechanism ensures that only signed and trusted firmware is executed, while any unsigned or modified firmware is immediately rejected. This secure boot process forms the foundation of the system's defense against firmware-level attacks.

The system also incorporates a secure communication layer based on the MAVLink 2.0 protocol with message signing enabled. This layer facilitates communication between the UAV and the Ground Control Station (GCS) or companion computer through telemetry links. By integrating cryptographic message validation, the system prevents unauthorized command injection and ensures that only authenticated messages are processed.

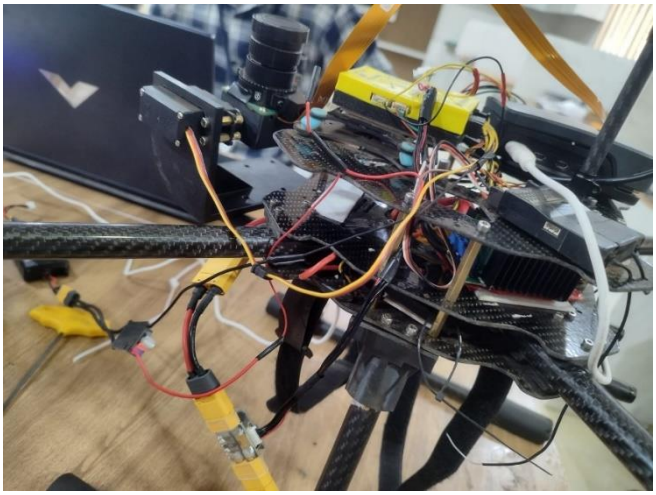

Fig. 1. Hardware of Secure UAV

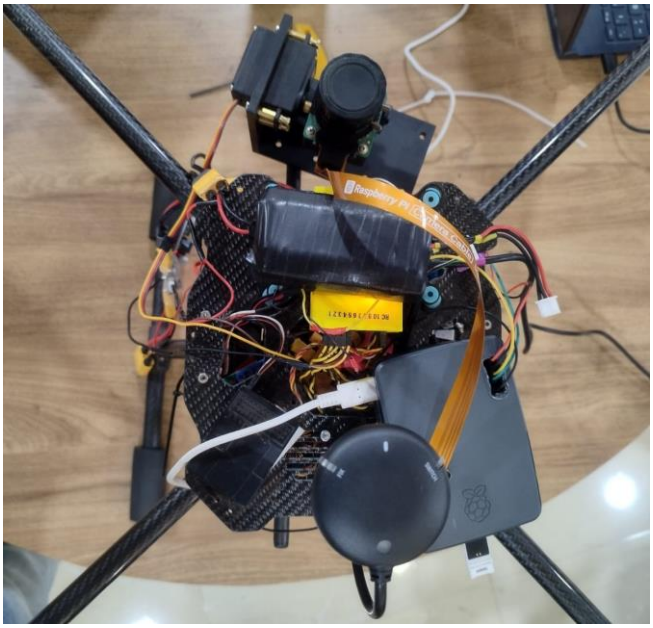

Fig. 2. Hardware of Secure UAV

A key component of the proposed system is the **authorized key check module**, which provides runtime security for parameter access. This module intercepts all parameter update requests and enforces a challenge-response authentication mechanism using cryptographic keys. When a user attempts to modify UAV parameters, the system generates a nonce and requires a valid signed response before granting access. This ensures that only authorized users can modify critical flight parameters, while unauthorized attempts are rejected and handled securely.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

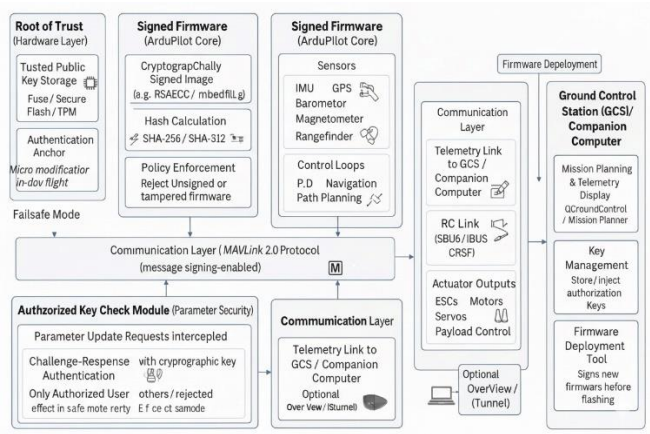

Fig. 3. Architecture of Secure UAV

The control and sensing subsystem includes standard UAV components such as IMU, GPS, barometer, and magnetometer, which provide real-time flight data. These sensors work in conjunction with control algorithms responsible for navigation, path planning, and stabilization. The actuator subsystem, including ESCs, motors, and servos, executes control commands generated by the flight controller.

On the ground side, the Ground Control Station (GCS), such as Mission Planner or QGroundControl, is used for mission planning, telemetry monitoring, and secure parameter management. A dedicated key management mechanism is used to securely store and inject authorization keys required for authentication. Additionally, a firmware deployment tool ensures that all firmware updates are signed before being uploaded to the UAV.

Overall, the proposed system integrates secure boot, encrypted communication, and authenticated access control into a unified framework. By combining hardware-based trust with software-level cryptographic enforcement, the system provides a robust solution for protecting UAVs against firmware tampering, unauthorized access, and communication-based attacks.

IV. METHODOLOGY

The proposed secure UAV framework follows a structured methodology designed to preserve firmware integrity, prevent unauthorized access, and strengthen the overall security of the system. The complete approach is organized into three key stages: Firmware Signing, Secure Boot Verification, and Runtime Authentication. Together, these stages establish a layered security model that safeguards both the UAV firmware and its communication channels.

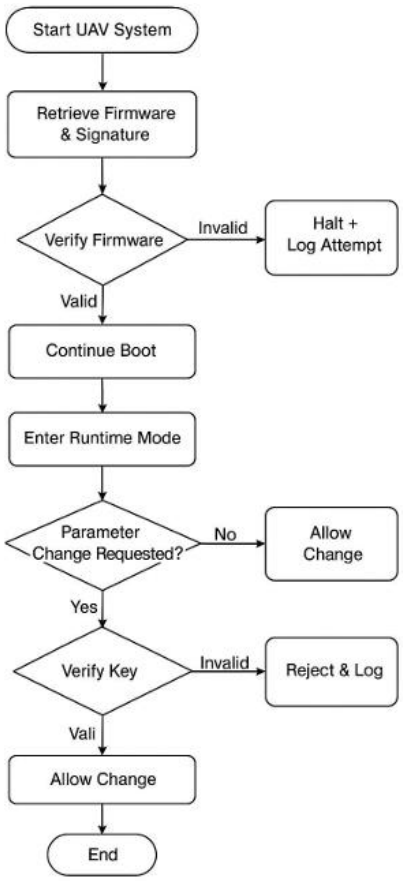

Fig. 4. Flowchart of Secure UAV

To maintain firmware authenticity, the system combines asymmetric cryptography with hashing and digital signature techniques. The SHA-256 algorithm is employed to generate a unique cryptographic digest of the firmware binary. It processes the firmware data through multiple rounds of hashing to produce a 256-bit hexadecimal output that uniquely represents the contents of the file. Even a minor modification within the firmware results in a completely different hash value, making unauthorized changes easy to detect. Owing to its collision resistance and computational efficiency, SHA-256 is particularly suitable for resource-constrained embedded platforms such as UAV flight controllers.

A. FIRMWARE SIGNING PHASE(OFFLINE PHASE)

The firmware signing process is carried out during development before the firmware is deployed onto the UAV. Initially, the firmware is compiled using the ArduPilot framework to generate the executable binary. A SHA-256 hash of this binary is then computed as:

$$H=SHA256(Firmware)$$

The resulting has serves as a unique fingerprint of the firmware image. This digest is subsequently encrypted using the developer's private key to generate a digital signature:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

$$S=Encrypt(H,Kpriv)$$

The generated signature provides authenticity and non-repudiation, confirming that the firmware originates from a trusted source. The final deployment package consists of the firmware binary, its digital signature, and the associated public key. This public key is securely stored within the UAV and later used during the verification process at startup.

B. SECURE BOOT VERIFICATION PHASE

The secure boot procedure is initiated each time the UAV is powered on. Its purpose is to validate the integrity and authenticity of the firmware before execution. During this phase, the bootloader retrieves the firmware image, the stored signature, and the embedded public key. A fresh hash of the firmware is generated using SHA-256:

$$H'=SHA256(Firmware)$$

Simultaneously, the stored digital signature is decrypted using the public key to retrieve the original hash:

$$H=Decrypt(S,Kpub)$$

The system compares the newly generated hash with the decrypted hash. If both values match, the firmware is verified as genuine and execution proceeds normally. Any mismatch indicates possible tampering, prompting the boot process to terminate immediately. This mechanism ensures that unauthorized or malicious firmware cannot be executed. In addition, verification failures are recorded for future analysis and investigation.

C. RUNTIME AUTHENTICATION PHASE

To further strengthen operational security, the proposed framework incorporates a runtime authentication mechanism that restricts unauthorized modifications to UAV parameters. This stage employs a challenge-response protocol based on nonces and digital signatures. Whenever a Ground Control Station (GCS) requests access to modify flight parameters, the UAV generates a random 32-byte nonce that serves as a unique authentication challenge. The nonce is transmitted to the GCS through MAVLink communication. Upon receiving this challenge, the GCS signs the nonce using its private key:

$$Sig=Sign(Nonce,Kpriv)$$

The signed nonce is then transmitted back to the UAV. The UAV verifies this signature using the stored public key:

$$Verify(Sig,Nonce,Kpub)$$

Successful verification confirms the identity of the requesting user and grants access to parameters modification. If verification fails, the request is rejected and logged as an unauthorized access attempt. This process guarantees that only authenticated users possessing valid credentials can alter critical system settings.

D. MAVLINK-BASED COMMUNICATION INTEGRATION

The authentication framework is integrated into the UAV architecture through MAVLink communication. Customized MAVLink commands facilitate secure interactions between the Ground Control Station and the flight controller. One command is responsible for requesting the nonce, while another confirms successful authentication. This approach maintains compatibility with existing Ground Control Stations and avoids extensive modifications to the underlying communication protocol.

E. LOGGING AND SECURITY ENFORCEMENT

To maintain traceability and support forensic analysis, the system incorporates a logging mechanism that records all critical events. These include firmware verification results, authentication attempts, and unauthorized access incidents. Logs are stored in onboard memory and can be retrieved via the Ground Control Station. This feature enhances system transparency and aids in identifying potential security threats.

IV. RESULT AND ANALYSIS

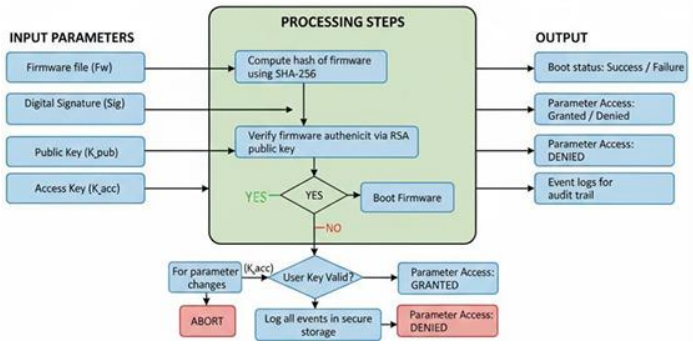

Fig. 5. Analysis Model of Secure UAV

This diagram illustrates a secure firmware boot and access control process for a system like a UAV. The INPUT PARAMETERS include the Firmware file (Fw), Digital Signature (Sig), Public Key (Kpub), and Access Key (Kacc). The PROCESSING STEPS first compute the firmware's hash using SHA-256 and then verify its authenticity using the RSA public key against the digital signature. If verification is successful (YES), the system outputs Boot status: Success and proceeds to Boot Firmware. If verification fails (NO), the process checks if a parameter change is being attempted. For parameter changes, the system checks if the User Key is Valid; if

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

valid, Parameter Access is GRANTED; if invalid, or if the initial boot failed, it logs all events and outputs Boot status: Failure or Parameter Access: DENIED. The overall process generates several OUTPUT states, including event logs for an audit trail.

The proposed secure UAV framework was implemented and tested using ArduPilot firmware integrated with cryptographic authentication mechanisms. The results obtained from the system validate the effectiveness of both firmware-level protection and runtime access control.

A. FIRMWARE SIGNING AND INTEGRITY VERIFICATION

The firmware signing process was successfully executed during the build stage, where the firmware binary was hashed and digitally signed using cryptographic keys. The implementation output confirms that the signing process was completed without errors, ensuring that only authenticated firmware is deployed onto the UAV. This step establishes the foundation for secure boot verification and prevents unauthorized firmware from being executed.

B. RUNTIME AUTHENTICATION AND AUTHORIZATION

The runtime authentication mechanism was tested using a nonce-based challenge-response protocol. Upon initiating authentication, the UAV generates a random nonce, which is transmitted to the Ground Control Station. The GCS signs the nonce using its private key and sends the response back to the UAV.

As observed in the implementation output, the system successfully verifies the digital signature and displays an “Authentication Successful” message, indicating that the session is authorized. This confirms that the authentication mechanism is functioning correctly and ensures that only legitimate users can access UAV parameters.

C. UNAUTHORIZED ACCESS PREVENTION

Before authentication, attempts to modify UAV parameters were intentionally made through the Ground Control Station. The system correctly blocked these requests and returned error messages such as “not authorized” or parameter update failure. This behavior demonstrates that the access control mechanism is actively enforcing security policies and preventing unauthorized configuration changes.

D. AUTHORIZED PARAMETER MODIFICATION

After successful authentication, the same parameter modification operations were performed. The system allowed these changes without any errors, confirming that access control is conditionally granted based on successful cryptographic verification. This clearly illustrates the effectiveness of the authentication layer in differentiating between authorized and unauthorized users.

E. SYSTEM PERFORMANCE AND OVERHEAD

The integration of cryptographic mechanisms introduced minimal performance overhead. The secure boot verification process resulted in a negligible delay during system startup, estimated to be within acceptable limits for embedded UAV systems. Similarly, the runtime authentication process was executed efficiently without noticeable latency in parameter updates. This demonstrates that the proposed system is lightweight and suitable for real-time UAV operations.

F. OVERALL SYSTEM EFFECTIVENESS

The experimental results confirm that the proposed system achieves its primary objectives of ensuring firmware integrity and enforcing secure access control. The combination of secure boot and runtime authentication provides a comprehensive defense mechanism against firmware tampering and unauthorized command execution. Compared to traditional UAV systems, which often lack such protections, the proposed approach significantly enhances system security while maintaining operational efficiency.

The expected outcome of this project was to design and implement a secure UAV system capable of resisting firmware tampering and preventing unauthorized configuration changes through cryptographic validation and access control mechanisms. The system was designed to ensure firmware authentication at boot time by verifying a digitally signed firmware, thereby rejecting any modified or unsigned code during startup. Additionally, a runtime access control mechanism was implemented to allow parameter modifications only after successful key-based authentication, with all unauthorized attempts being denied and logged. The system also maintains detailed logs of firmware verification events and access attempts to support post-flight analysis and system auditing. Furthermore, the security mechanisms were developed to be lightweight, ensuring minimal impact on system performance, with boot verification delays maintained within acceptable limits (typically under 2 seconds). Finally, the solution was designed to be scalable and compatible with open-source UAV platforms such as ArduPilot, making it adaptable to similar autopilot hardware like PX4.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

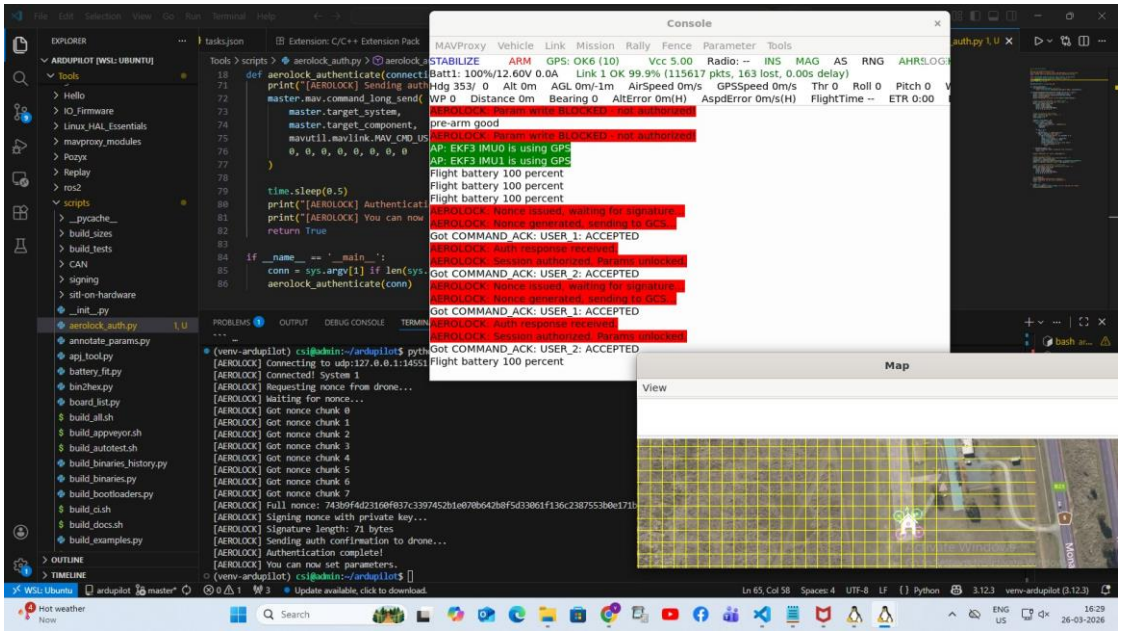

Fig. 6. Implementation of Securing firmware

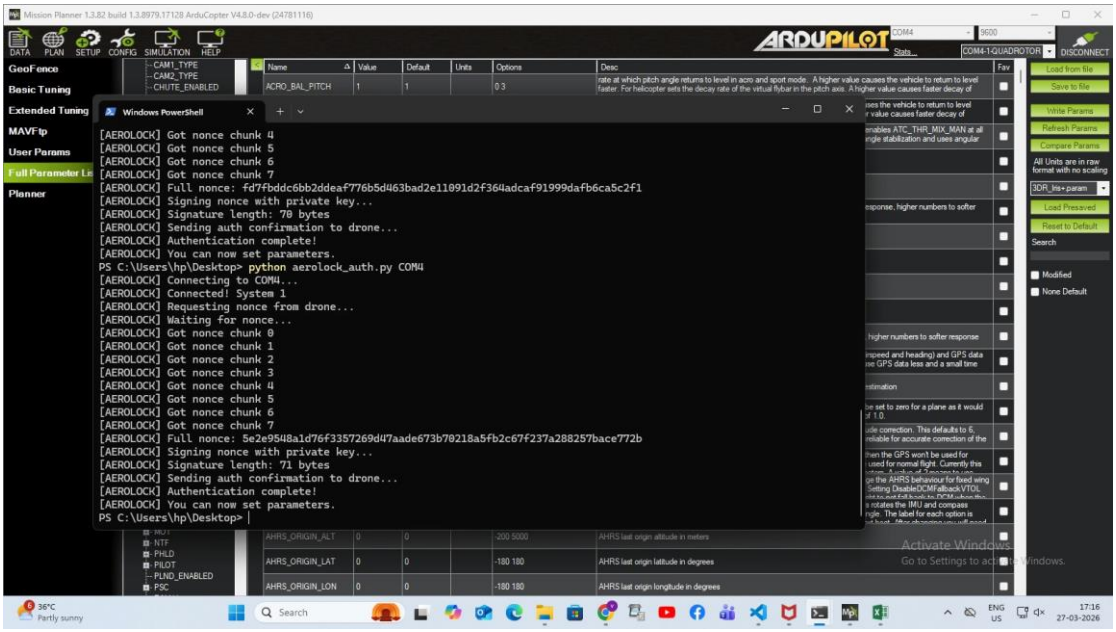

Fig. 7. Implementation of Securing firmware(The nonce chunks shows the key)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

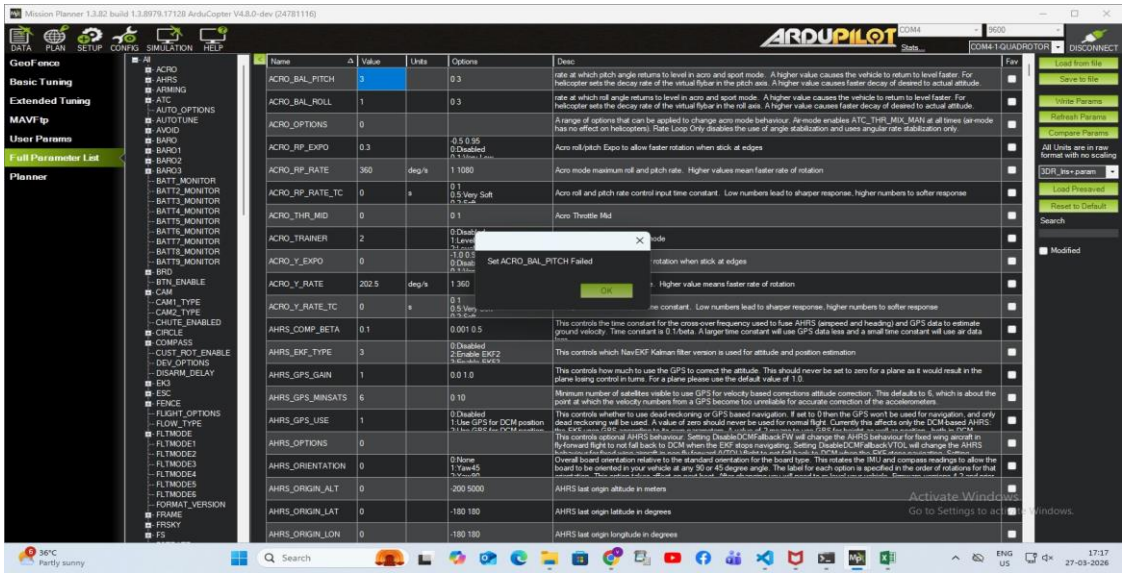

Fig. 8. Implementation of Securing firmware(Parameter changing failed due to unauthorised Access)

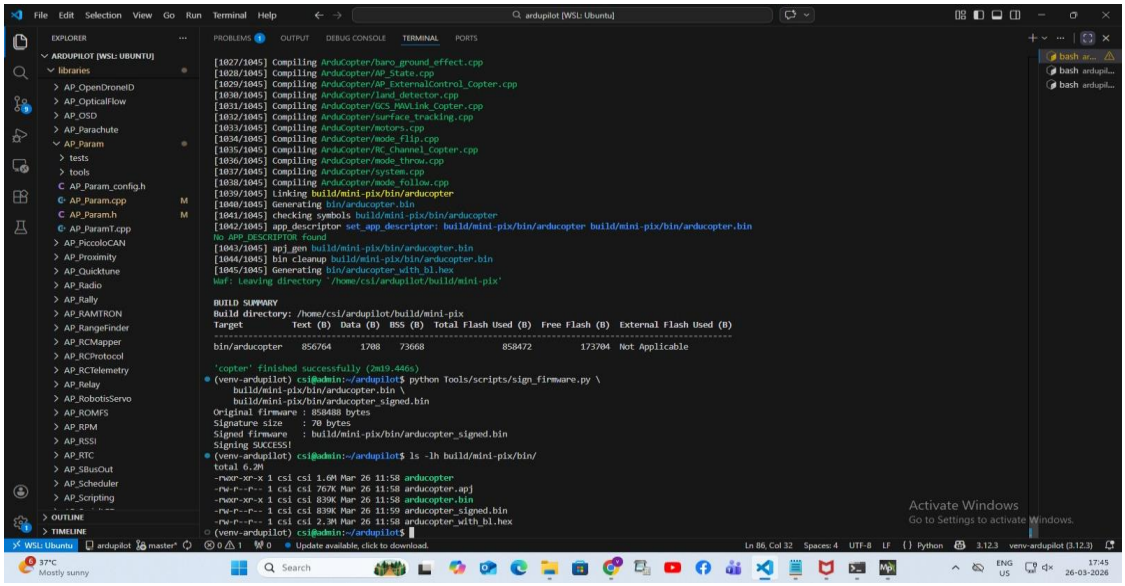

Fig. 9. Implementation of Securing firmware

V. DISCUSSION

The implementation of the proposed secure UAV framework demonstrates the effectiveness of integrating cryptographic techniques for enhancing firmware security and access control in embedded aerial systems. The results obtained from the system indicate that the incorporation of encryption-based secure boot and authentication mechanisms significantly improves the resilience of UAVs against firmware-level attacks and unauthorized access.

The secure boot mechanism successfully ensures firmware integrity by validating the digital signature before execution. During testing, it was observed that any modification in the firmware results in a mismatch in the computed hash and the decrypted signature, thereby preventing the UAV from booting. This confirms that the system effectively detects tampered or unauthorized firmware, eliminating the possibility of executing malicious code. This behavior aligns with the expected outcome of cryptographic integrity verification and demonstrates the reliability of the SHA-256 and asymmetric encryption-based approach.

In addition to boot-time security, the runtime authentication mechanism introduces an extra layer of protection by restricting parameter modifications to authorized users only. The implemented challenge-response protocol using nonce-based authentication ensures that each authentication attempt is unique and resistant to replay attacks. The system successfully validates the authenticity of the Ground Control Station by verifying digitally signed responses, thereby preventing unauthorized command injection through MAVLink communication. This is particularly significant as it addresses a critical vulnerability in traditional UAV

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

systems where parameter modification is often unprotected.

From a performance perspective, the integration of cryptographic operations introduces a minimal overhead in system startup time. The observed delay during boot is negligible (approximately 1–2 seconds) and does not impact the operational efficiency of the UAV. This indicates that the proposed solution is lightweight and suitable for resource-constrained embedded platforms such as Pixhawk controllers. Furthermore, the runtime authentication process does not introduce noticeable latency during parameter updates, ensuring seamless user interaction.

The logging and monitoring mechanism further strengthens the system by maintaining a record of all security-related events, including firmware verification status and authentication attempts. This feature enhances system transparency and enables post-operation analysis, which is essential for identifying potential security breaches and improving system reliability.

Overall, the results demonstrate that the proposed system effectively combines secure boot and runtime authentication to provide a comprehensive security framework for UAVs. Compared to existing approaches that focus only on firmware validation or communication security individually, this integrated approach offers a more robust and practical solution. The implementation on a real-world platform such as ArduPilot further validates the feasibility and applicability of the proposed system in real-world UAV deployments.

VI. CONCLUSION

In this project, a secure and tamper-resistant UAV firmware system was successfully designed and implemented to address increasing cybersecurity threats in UAV operations.

The proposed system integrates a secure boot mechanism using RSA (asymmetric cryptography) and SHA-256 hashing to verify firmware integrity before execution. It also introduces a key-based access control layer to prevent unauthorized parameter modifications during runtime.

Testing conducted on the Pixhawk controller and Mission Planner environment confirmed that the system effectively prevents the execution of tampered firmware, maintains full operational stability, and achieves high reliability with minimal performance overhead (~1.6 seconds boot delay).

The project demonstrates how cybersecurity principles can be embedded within UAV firmware, ensuring safe and trustworthy operation in mission-critical environments such as defense, agriculture, and surveillance.

The scope of this project is centered on enhancing the security and reliability of UAV firmware through the integration of cryptographic mechanisms and runtime access control.

REFERENCES

[1] Aaron Yu, Iuliia Kolotylo, Hashim A. Hashim and Abdelrahman E. E. Eltoukhy, " Electronic Warfare Cyberattacks, Countermeasures, and Modern Defensive Strategies of UAV Avionics," IEEE Access, 2025.

[2] Ioannis Anagnostis, Panayiotis Kotzanikolaou, Christos Douligeris, " Understanding and Securing the Risks of Uncrewed Aerial Vehicle Services," IEEE Access, 2025.

[3] Yuanxu Zhu, Tianze Zhang, Aiying Wu, and Gang Shi, “PISCFF-LNet: A Method for Autonomous Flight of UAVs Based on Lightweight Road Extraction,” 10.3390/drrones9030226, 20 March 2025.

[4] Alessandro Erba, John H. Castellanos, Sahil Sihag, Saman Zonouz and Nils Ole Tippenhauer, "Sensor Deprivation Attacks for Stealthy UAV Manipulation," arXiv, 2024.

[5] D. Wanner, H. A. Hashim, S. Srivastava, and A. Steinhauer, “UAV avionics safety, certification, accidents, redundancy, integrity, and reliability: A comprehensive review and future trends,” Drone Syst. Appl., vol. 12, pp. 1-23, Jan 2024.

[6] A. Rugo, C. A. Ardagna, N. E. Ioini — A Security Review in the UAVNet Era: Threats, Countermeasures, and Gap Analysis, ACM Computing Surveys, 2023.

[7] Z. Lv, Y. Li, J. Wu, H. Lv — Securing the Internet of Drones Against Cyber-Physical Attacks, IEEE Internet of Things Magazine, 2021.

[8] Khamvilai, J. Dunham, E. Feron, and E. N. Johnson, “Avionics of aerial robots,” Current Robot. Rep., vol. 2, no. 2, pp. 113-124, June 2021.

[9] Z. Lv, Y. Li, J. Wu, and H. Lv, “Securing the Internet of Drones against cyber Physical attacks,” IEEE Internet Things Mag., vol. 4, no. 4, pp. 74-78, Dec 2021.

[10] M. Leonardi, M. Strohmeier, and V. Lenders, “On jamming attacks in crowdsourced Air traffic surveillance,” IEEE Aerosp. Electron. Syst. Mag., vol. 36, no. 6, pp. 44-54, June 2021.

[11] V. P. Riabukha, “Radar surveillance of unmanned aerial vehicles,” Radioelectronics Commun. Syst., vol. 63, no. 11, pp. 561-573, 2020.

[12] Dong Yang, Wei Dong, Wei Lu, Yanqi Dong, and Sirui Liu – Vulnerabilities Analysis and Secure Controlling for Unmanned Aerial System Based on Reactive Synthesis, VOL. 14 NO. 8, August 2015.

[13] J. Gu, T. Su, Q. Wang, X. Du, and M. Guizani, “ Multiple moving targets surveillance Based on a cooperative network for multi-UAV,” IEEE Commun. Mag., vol. 56, no. 4, pp. 82- 89, April 2018.

[14] K. Hartmann, C. Steup — The Vulnerability of UAVs to Cyberattacks — A Risk Assessment Approach, CYCON Conference, 2013.

Author Biographies

ARCHANA KOTAKAR has completed her Bachelor’s degree in Electronics and Telecommunication Engineering from Savitribai Phule Pune University and her Master’s degree in VLSI System Design from Jawaharlal Nehru Technological University (JNTU). She is currently pursuing her Ph.D. at Vel Tech University. She is presently working as an Assistant Professor at JSCOE, Pune.

VISHAL GAJANAN ZALAKE is currently in the final year of his Bachelor of Engineering degree in Computer Engineering at Savitribai Phule Pune University, Pune, India, expected to graduate in 2026. He is currently undertaking a full-time internship at CerebroSpark Innovations Pvt. Ltd. His research interests include hardware and firmware design and optimization, authorization, and implementation.

VAISHNAVI VIVEK SARAF is currently in the final year of her Bachelor of Engineering degree in Computer Engineering at Savitribai Phule Pune University, Pune, India, expected to graduate in 2026. She is currently undertaking a full-time internship at CerebroSpark Innovations Pvt. Ltd. Her research interests include firmware design and optimization, cryptographic encryption, and implementation.

RADHEY PARIKSHIT BILDIKAR is currently in the final year of his Bachelor of Engineering degree in Computer Engineering at Savitribai Phule Pune University, Pune, India, expected to graduate in 2026. His research interests include firmware design and optimization, cryptographic encryption, and implementation.

SMITESH VIVEK SHINDE is currently in the final year of his Bachelor of Engineering degree in Computer Engineering at Savitribai Phule Pune University, Pune, India, expected to graduate in 2026. His reaerch interests include hardware design and optimization and implementation.