Next-Generation AI-Driven Cybersecurity Framework for Flying Taxis Using Intrusion Detection and Secure Command Validation

Mr. Y. Manohar Reddy[1], K. Dhruv Sharma[2], P. Gnan Aman[3], B. Sai Sri Vallabha[4]
[1]*Assistant Professor, Dept. of CSE-(CyS,DS) and AI & DS, VNR VJIET, Hyderabad, India*
[2,3,4]*Student, VNR VJIET, Hyderabad, India*

***Abstract*—Urban Air Mobility (UAM) operates as an advanced transportation system which enables cities with high population density to achieve better passenger movement outcomes while decreasing road traffic. The emerging ecosystem depends on flying taxis which are known as electric Vertical Take-Off and Landing (eVTOL) vehicles.**

The operation of these vehicles depends on digital technologies which include GPS navigation systems and wireless communication networks and automated flight control systems and cloud- based monitoring platforms.

The increasing use of digital systems that connect to each other makes flying taxi systems more vulnerable to various cyber security risks. Attackers may attempt to manipulate navigation signals through GPS spoofing, inject malicious commands into the flight control system, or launch network-based intrusions to disrupt communication channels. Cyber-attacks targeting these systems will result in severe security breaches which endanger passenger safety and cause operational disruptions and create risks of operational disasters.

The research introduces a next-generation AI-based cybersecurity framework which protects flying taxi systems by reinforcing both their security measures and operational reliability. The security system uses machine learning technology to build an Intrusion Detection System (IDS) which detects unauthorized access attempts while deep learning technology creates an autoencoder model to detect GPS spoofing. The system uses RSA encryption to secure communications between different system components while verifying command execution through encrypted command validation.

The security alert system uses a dashboard which provides real-time information about security alerts and system health status and system alerts which show detected attack patterns. Index Terms—Urban Air Mobility, Flying Taxi Security, UAV Cybersecurity, Intrusion Detection System, GPS Spoofing Detec- tion, Autoencoder, RSA Encryption

***Index Terms*—Urban Air Mobility, Flying Taxi Security, UAV Cybersecurity, Intrusion Detection System, GPS Spoofing Detection, Autoencoder, RSA Encryption**

I. INTRODUCTION

Urban Air Mobility represents a revolutionary transformation in modern transportation infrastructure. As urban environments experience population growth, the efficiency of existing road-based transportation systems suffers from in-creasing congestion problems. Flying taxis powered by electric vertical take-off and landing technology have been proposed as an innovative solution to address these challenges. Flying taxi systems depend on multiple high-tech components which include GPS navigation systems and wireless communication networks and automated control systems and cloud-based monitoring platforms. The implementation of these technologies creates cybersecurity weaknesses which attackers can use to their advantage. GPS spoofing attacks, malicious command injection, and network intrusions are some of the major threats that can compromise flight safety and disrupt aerial transportation systems. This research proposes an integrated AI-driven cybersecurity framework capable of detecting cyber threats and ensuring secure communication in flying taxi systems.

II. RELATED WORK

Several researchers have explored cybersecurity challenges associated with modern UAV and aviation

systems.
Ekstro¨m conducted a comprehensive review of cybersecurity risks affecting airline operations and emphasized the growing importance of digital security in aviation infrastructure.

TP et al. presented a detailed review of urban air mobility technologies and discussed the rapid development of air taxis and drone-based transportation systems.

Saifudeen et al. analyzed the evolution of electric vertical take-off and landing aircraft and highlighted cybersecurity as a major challenge for future aerial transportation.

Popli et al. proposed a federated learning-based intrusion detection system for distributed UAV networks.

Zhang et al. developed a lightweight authentication system which uses federated learning and zero-trust principles to enhance UAV communication security. The research studies deliver important findings about UAV security yet existing studies concentrate on studying individual security technologies instead of developing comprehensive cybersecurity systems.

III. METHODOLOGY

The proposed cybersecurity framework follows a multi-layer security architecture design process that enables detection and defense against cyber-attacks which target flying taxi systems. The system uses machine learning models together with encrypted communication systems and real-time monitoring tools to deliver secure and dependable aerial transportation service. The system operates by collecting operational data from the flying taxi system while it analyzes communication traffic to identify malicious activities and validates commands through secure cryptographic mechanisms and generate alerts whenever they identify security threats. The methodology is represented through a set of system design diagrams which in- clude system architecture and use case diagram and workflow diagram and sequence diagram.

A. System Architecture

The system architecture shows how the proposed cybersecurity framework will function while showing how its various components will work together. The architecture includes the operator interface, back- end processing server, machine learning modules for intrusion detection and GPS spoofing detection, secure command vali- dation mechanisms, and the flying taxi control system. The operator interacts with the system through a monitoring dashboard which provides real- time information about system health and potential cyber threats. The backend server processes incoming data streams from the flying taxi system and forwards them to the appropriate security modules for analysis. The intrusion detection system analyzes network communication patterns to identify suspicious traffic, while the GPS spoofing detection module monitors navigation signals for anomalies. Secure command validation ensures that only authenticated commands are executed by the flying taxi control system.

B. Use Case Diagram

The use case diagram shows how the system operator interacts with the cybersecurity framework. The operator can monitor system activity, observe security alerts, and analyze detected cyber threats through the monitoring dashboard. The system performs multiple security operations which include monitoring network traffic and detecting GPS signal anomalies and validating commands through cryptographic authentication and creating system activity logs. The flying taxi system uses these functions to protect itself from multiple cyber threats.

C. Workflow Diagram

The workflow diagram shows the cybersecurity framework operational process through its step-by-step demonstration. The flying taxi system starts by gathering system data which includes GPS signals and network traffic. The system sends this data to the backend processing server, which performs data analysis. The intrusion detection module evaluates network communication patterns to detect network traffic that shows unusual behavior.

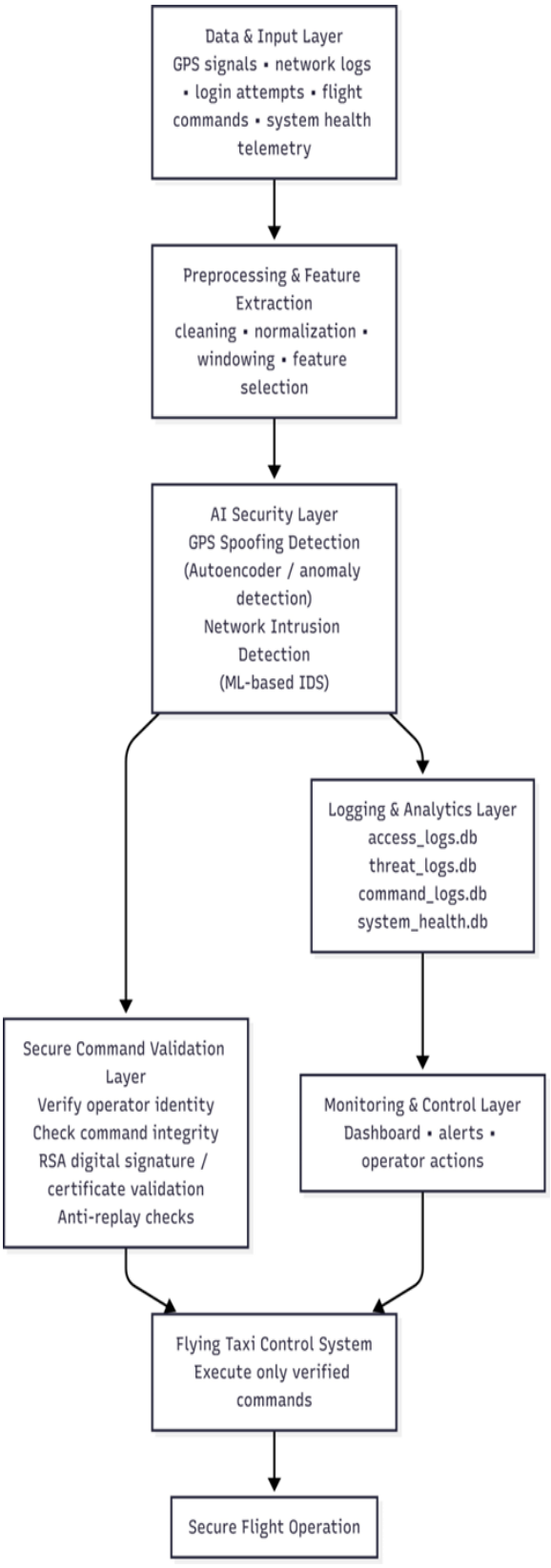

Fig. 1. System Architecture of the Proposed Cybersecurity Framework

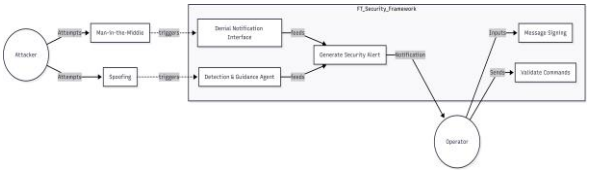

Fig. 2. Use Case Diagram of the Flying Taxi Cybersecurity System

The GPS spoofing detection module uses a trained au- toencoder model to analyze navigation signals and detect anomalies. The system produces alerts when it detects suspicious activity, which it records in the database for future investigation.

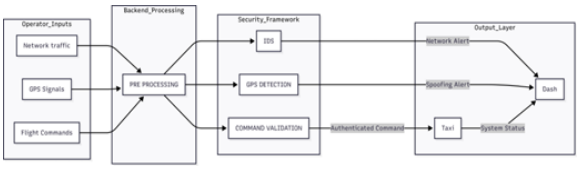

Fig. 3. Workflow of the AI-driven Cybersecurity Framework

D. Sequence Diagram

The sequence diagram shows how system components inter- act with each other through their regular operations and their cyber- attack detection procedures. The operator dashboard command gets sent to the secure command validation module which first checks the command through RSA encryption be- fore it proceeds to the flying taxi control system for execution. The system operates through two monitoring systems which check for both current system operations and potential GPS spoofing attacks. The system generates immediate alerts while it creates system logs to document the occurrence of a cyber threat detection.

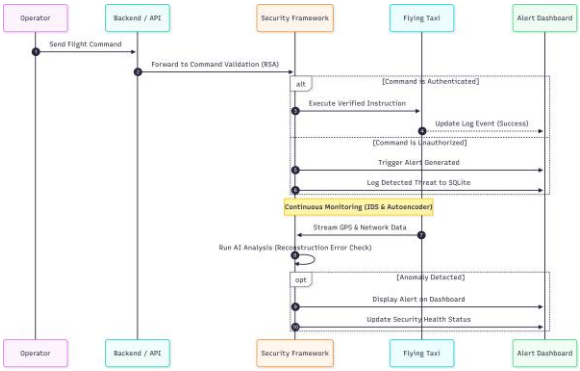

Fig. 4. Sequence Diagram Showing Interaction Between System Components

IV. PROPOSED SYSTEM

Different security measures are combined together in the provision of a security framework to be addressed in detecting and countering cyber-attacks" in flying taxi systems.

A. GPS Spoofing Detection

The researchers developed GPS spoofing detection through their implementation of a deep learning autoencoder model. The model learns patterns of legitimate GPS signals and detects anomalies using reconstruction error.

$Loss = ||X - \hat{X}||^2$

When the likely value is smaller than previously established thresholds, the system alerts the traffic intelligent of a spoofing signal.

B. Intrusion Detection System

The intrusion detection system observes network traffic which travels between the flying taxi and the ground control system. The system uses machine learning algorithms to detect network abnormalities and identify suspicious traffic patterns.

C. Secure Command Validation

The system uses RSA-based encryption to protect against unauthorized command injection attacks by verifying command authentication. The flying taxi control system permits only execution of commands that have been verified through testing.

D. Logging and Monitoring

The centralized database stores all detected threats and system activities. The monitoring dashboard shows real-time alerts together with system status and attack history.

V. IMPLEMENTATION

The proposed cybersecurity framework needs to be implemented through the combination of different software systems and machine learning algorithms which will identify cyber threats against flying taxi operations. The system backend is constructed through Python programming with the Flask framework as its foundation.

Flask serves as the communication link which connects the frontend dashboard to the security modules. The system manages API requests while handling incoming data streams and directing different cybersecurity elements throughout their operational processes.

The Scikit-Learn library functions as the foundation for implementing machine learning models which detect intrusion attempts. The models use network data to identify standard network behavior and detect suspicious activities. The model uses training data which contains examples of both valid network traffic and security attack patterns.

The system uses TensorFlow to create a deep learning autoencoder model which detects GPS spoofing. The autoencoder trains itself to identify standard navigation behavior by using authentic GPS signals. The system uses the autoencoder model to analyze all incoming GPS signals during its active period.

The system detects a signal as abnormal when its reconstruction error surpasses the set threshold which triggers the system to issue a spoofing alert. The system uses RSA-based encryption methods to establish command authentication procedures. When an operator sends a command through the dashboard the command goes through an encryption and verification process before the flying taxi control system executes it.

This process guarantees that only authorized users can make changes to flight operations through command execution. The system implements a central logging system which operates through SQLite databases. The database stores all identified threats along with system operations and alerts which will be used for monitoring purposes and subsequent analysis. A web-based monitoring dashboard system displays real-time operational information through online access.

VI. RESULTS AND DISCUSSION

The developed prototype demonstrates the effectiveness of the proposed cybersecurity framework in detecting cyber at- tacks targeting flying taxi systems. The researchers conducted multiple experiments to test how well the system could detect harmful activities and produce security alerts during real-time operations.

A. GPS Spoofing Detection

The GPS spoofing detection module uses a deep learning autoencoder model to analyze navigation signal patterns. The model is trained using legitimate GPS data to learn normal flight navigation behavior. The system detects an anomaly when manipulated or spoofed GPS signals enter the system because the autoencoder generates an increased reconstruction error.

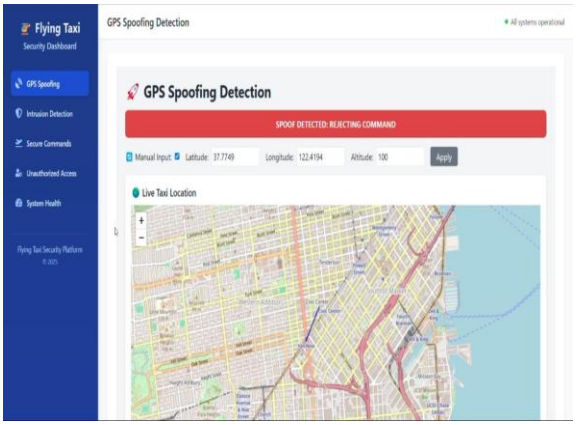

Fig. 5. Detection of GPS Spoofing Attack

The monitoring dashboard displays alerts when the system detects unexpected GPS tracking patterns. The system enables the operator to detect navigation system manipulation attempts at any moment.

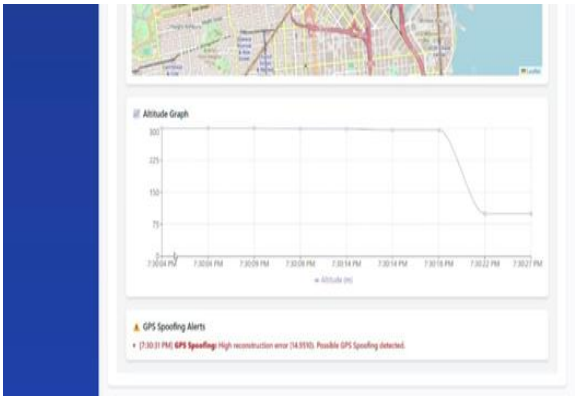

Fig. 6. GPS Signal Anomaly Detection Interface

B. Intrusion Detection System

The intrusion detection system keeps track of network traffic between the flying taxi system and its backend server. The system uses machine learning algorithms to examine traffic patterns and detect any abnormal communication activities.

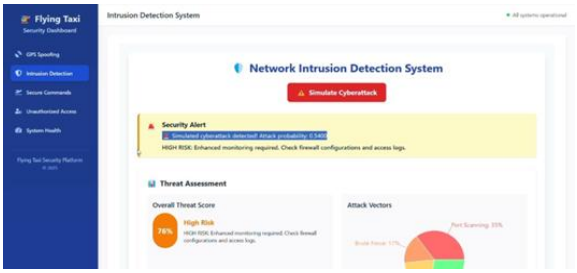

Fig. 7. Intrusion Detection Alert Generated by the System

The system raises alarms on anomalies in traffic and logs events for further examination.

C. Secure Command Validation

The flying taxi control system executes only authenticated commands through its secure command validation process. The RSA encryption mechanism verifies command authentic- ity before forwarding it to the flight controller.

This mechanism prevents attackers from injecting unauthorized commands into the system.

D. System Logs and Monitoring

The system keeps detailed records of all security incidents and all detected threats and all system operations. The monitoring dashboard shows the logs which are stored in a database.

The operator can analyze the previous security events, observe the patterns of attack, and support the operator foroperational security situation raising in the taxo system.

VII. CONCLUSION

Urban Air Mobility is anticipated to become a major element of future transportation systems because it offers fast and dependable travel solutions for busy city areas.and verified commands are executed by the flying taxi control system.

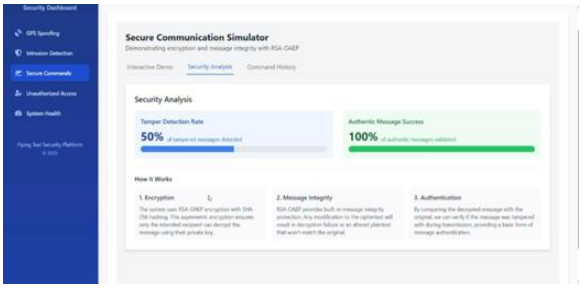

Fig. 8. Secure Command Authentication Interface

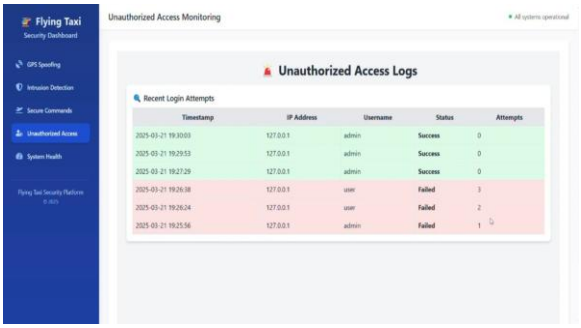

Fig. 9. System Logs and Security Monitoring Dashboard

Flying taxis that use electric Vertical Take-Off and Landing (eVTOL) systems serve as essential elements of this future plan. The operation of these systems depends excessively on digital technologies which include GPS navigation and wire- less communication networks and automated control systems. GPS spoofing and malicious command injection and net- work intrusion attacks create security risks which can damage flight safety and interrupt aerial transportation operations. The research established an all-embracing cybersecurity system using artificial intelligence methods which protects flying taxi systems with enhanced security and dependable operation capabilities.

The system design includes different security components which use a machine learning-based Intrusion Detection Sys- tem and a deep learning autoencoder model for GPS spoofing detection and an RSA- based command validation mechanism to secure system component communication. The framework unifies security modules through its consolidated structure which enables detection of cyber threats and protection against unauthorized system access. The system architecture enables secure authentication of operational commands while monitoring all communication traffic and navigation signals. The intrusion detection system monitors network traffic to find un- usual behaviors which the system uses for detecting irregular system uses. The autoencoder-based model detects anomalies in GPS signals that may indicate spoofing attacks. The secure command validation module ensures that only authenticated

REFERENCES

[1] E. Ekstro¨m, “Cybersecurity challenges to airlines: A literature review of risk and compliance,” 2025.
[2] K. K. TP et al., “Urban Air Mobility: A comprehensive literature review on the growth of air taxis and drone delivery systems,” 2025.
[3] O. A. Saifudeen et al., “The ongoing evolution of EVTOLs: urban transport potential and the security dimension,” 2025.
[4] V. Karadzhov and R. Yuleva-Chuchulayna, “Virtual Security Risks During Tourist Travel.”
[5] I. Suarez, “The Future of Transportation – Emerging Self-driving Taxis,” 2025.
[6] A. Nova´k and E. Nica, “Urban drone mobility solutions enabling air taxis logistics.”
[7] A. Phadke and N. Majumdar, “Towards personal aerial vehicles for urban air mobility transportation.”
[8] M. S. Popli et al., “Federated learning framework for cyber intrusion detection.”
[9] A. Al Farsi et al., “Privacy and security challenges in federated learning for UAV systems.”
[10] H. Zhang et al., “Federated learning-based lightweight network with zero trust for UAV authentication.”
[11] Y. Shoukry, A. Puggelli, P. Nuzzo, A. L. Sangiovanni-Vincentelli, and P. Tabuada, “Secure state estimation for cyber-physical systems under sensor attacks,” IEEE Transactions on Automatic Control, vol. 62, no. 10, pp. 4917–4932, 2017.
[12] H. Sedjelmaci and S. M. Senouci, “Intrusion detection and prevention framework for UAV-based networks,” in Proc. IEEE Global Communi- cations Conference (GLOBECOM), 2015.
[13] M. Strohmeier, V. Lenders, and I. Martinovic, “On the security of the Automatic Dependent Surveillance–Broadcast protocol,” IEEE Commu- nications Surveys & Tutorials, vol. 17, no. 2, pp. 1066–1087, 2015.
[14] A. Humayed, J. Lin, F. Li, and B. Luo, “Cyber-physical systems security—A survey,” IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1802–1831, 2017.
[15] K. Hartmann and C. Steup, “The vulnerability of

UAVs to cyber- attacks—An approach to the risk assessment," in Proc. International Conference on Cyber Conflict (CyCon), 2013.

[16] T. Humphreys, "Detection strategy for cryptographic GNSS anti- spoofing," IEEE Transactions on Aerospace and Electronic Systems, vol. 49, no. 2, pp. 1073–1090, 2013.

[17] S. Bhunia and M. Tehranipoor, Hardware Security: A Hands-on Learn- ing Approach. Morgan Kaufmann, 2018.

[18] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 2, pp. 546–556, 2015.

[19] P. Paganini, "Cybersecurity challenges in drone technology," Cyber Defense Magazine, 2019.

[20] A. Ferdowsi and W. Saad, "Deep learning-based dynamic watermarking for secure signal authentication in UAV networks," in Proc. IEEE International Conference on Communications (ICC), 2018.

[21] S. Raju, Y. Manohar Reddy, K. Palaparthy, and J. Victor Paul, "Enhanc- ing Insider Threat Detection through Integrated Behavioral, Signature and Anomaly based Detection Methods."