IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

"OPTIMIZED PATH PLANNING FOR LAST-METER DRONE DELIVERY USING DEEP Q-NETWORKS"

[1] Mr. V.NAGA RAJU, [2] K VINOD KUMAR, [3] K THIRUMALESH, [4] B HEMANTH KUMAR,[5] K SAHITH REDDY

[1]Associate Professor, [2,3,4,5] UG STUDENT

[1,2,3,4,5]ELECTRONICS AND COMMUNICATION ENGINEERING(ECE)

[1,2,3,4,5] AVANTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY

Gunthapally(V), Abdullapurmet(M), R.R Dist - 501512. www.avanthi.edu.in

Abstract: The Optimized Path Planning for Last-Meter Drone Delivery Using Deep Q-Networks system is an intelligent autonomous delivery framework designed to improve the efficiency, speed, and reliability of last-meter logistics. Traditional delivery methods are often hampered by traffic congestion, high fuel consumption, increasing labour costs and delays in delivery, especially in congested urban areas and remote areas. To overcome these limitations, the proposed system employs Unmanned Aerial Vehicles (UAVs) with Deep Q-Network (DQN)-based reinforcement learning to achieve optimal path planning and autonomous navigation.

The system combines GPS navigation, real-time obstacle detection sensors, flight controllers, wireless communication technologies (RF/Wi-Fi/4G/5G), and a web-based management platform to execute safe and efficient package delivery. Unlike traditional shortest path algorithms, the DQN agent learns the optimal delivery route on the fly through interaction with the environment, taking into account dynamic obstacles, battery constraints, weather conditions, no-fly zones, and delivery priorities. This adaptive learning enables the drone to achieve minimal travel distance, energy consumption, and delivery time, whilst maximising delivery success and operational safety.

The proposed architecture is composed of hardware, software and communication layers and modules for user management, order processing, route optimisation, autonomous flight control, payload management, real-time tracking and monitoring. The system is implemented using Python, Flask, HTML, CSS and JavaScript and simulations are used to validate the effectiveness of the DQN based navigation strategy before implementation.

Experimental evaluation demonstrates that the proposed approach significantly improves route efficiency, reduces operational costs, decreases human intervention, and enhances delivery reliability compared to traditional ground-based logistics systems. Furthermore, the system is particularly suitable for medical supply transportation, emergency response, food delivery, grocery distribution, and e-commerce logistics, where rapid and contactless delivery is essential. The proposed framework is a scalable, eco-friendly and intelligent solution for future autonomous drone-based logistics, paving the way to smart last-meter delivery systems in modern cities and remote areas.

Keywords— Deep Q-Network (DQN), Last-Meter Drone Delivery, Path Planning, Reinforcement Learning, Unmanned Aerial Vehicle (UAV).

I. INTRODUCTION

The rapid growth of e-commerce, online retail services, and on-demand logistics has significantly increased the demand for faster, more reliable, and cost-effective delivery systems. Traditional last-mile delivery methods primarily rely on ground transportation, such as trucks, vans, and motorcycles, which are often affected by traffic congestion, road conditions, fuel costs, and labor shortages. These challenges lead to increased delivery time, higher operational expenses, and reduced customer satisfaction. As a result, there is a growing need for intelligent and autonomous delivery solutions capable of overcoming these limitations.

Drone technology has emerged as one of the most promising innovations for modern logistics and transportation. Unmanned Aerial Vehicles (UAVs) can travel through aerial routes, avoiding road traffic while providing rapid and contactless delivery services. Drone-based delivery systems are particularly valuable for transporting medical supplies, food, groceries, emergency equipment, and lightweight commercial goods. Their ability to reach remote and inaccessible locations makes them highly suitable for disaster management, healthcare logistics, and time-critical delivery applications.

Although drone delivery offers significant advantages, autonomous navigation remains one of the major challenges. A drone operating in real-world environments must determine an optimal flight path while avoiding obstacles, minimizing energy consumption, complying with flight restrictions, and adapting to changing environmental conditions. Conventional path-planning algorithms often struggle to handle dynamic environments efficiently because they rely on predefined routes and static optimization methods.

Recent advances in Artificial Intelligence (AI), particularly Reinforcement Learning (RL), provide an effective solution to this challenge. Deep Reinforcement Learning combines neural networks with reinforcement learning techniques to enable autonomous agents to learn optimal decision-making through continuous interaction with the environment. Among these techniques, the Deep Q-Network (DQN) algorithm has gained significant attention due to its capability to learn efficient navigation policies in complex and dynamic environments. Instead of following fixed routes, a DQN-based drone continuously evaluates environmental conditions and selects actions that maximize long-term rewards, resulting in shorter travel distances, lower energy consumption, improved safety, and faster deliveries.

The proposed project, "Optimized Path Planning for Last-Meter Drone Delivery Using Deep Q-Networks," presents an intelligent drone delivery framework that integrates Deep Q-Network-based path planning with GPS navigation, real-time obstacle detection, wireless communication, and autonomous flight control. The system enables drones to identify optimal delivery routes while considering battery constraints, weather conditions, obstacles, no-fly zones, and delivery priorities. It also incorporates a web-based interface that allows users to place delivery requests, monitor drone status, and track deliveries in real time.

The proposed architecture consists of three major layers: the hardware layer, software layer, and communication layer. The hardware layer includes the drone frame, brushless motors, propellers, Li-Po battery, GPS module, flight controller, sensors, and camera. The software layer is developed using Python, Flask, HTML, CSS, and JavaScript, providing intelligent route planning, user management, delivery scheduling, and monitoring functionalities. The communication layer ensures secure real-time data exchange between the drone and the control station through RF, Wi-Fi, or cellular networks, enabling continuous monitoring and autonomous decision-making.

The DQN-based path planning module forms the core of the proposed system. During training, the reinforcement learning agent interacts with a simulated environment where it learns optimal navigation policies by receiving rewards for reaching destinations safely and penalties for collisions, unnecessary energy consumption, and inefficient routes. Over time, the agent develops an optimized navigation strategy that significantly improves delivery efficiency compared to traditional shortest-path algorithms.

The proposed system offers numerous advantages over conventional delivery methods. It reduces delivery time by utilizing direct aerial routes, minimizes operational costs through automation, decreases dependency on human labor, and lowers carbon emissions by employing electric-powered drones. Furthermore, its real-time monitoring and adaptive route optimization capabilities enhance delivery reliability and operational safety.

The primary objective of this project is to develop an intelligent, autonomous, and scalable drone delivery system capable of optimizing last-meter logistics using Deep Q-Networks. By combining artificial intelligence, reinforcement learning, autonomous navigation, and modern web technologies, the proposed framework provides an efficient, secure, and environmentally sustainable solution for future smart logistics systems. The system has broad application potential in healthcare, emergency response, e-commerce, food delivery, grocery distribution, and disaster relief operations, making it a significant contribution toward the next generation of autonomous delivery technologies.

II.RELATED WORK:

Recent advances in Unmanned Aerial Vehicles (UAVs), Artificial Intelligence (AI), and Reinforcement Learning (RL) have greatly altered the field of autonomous drone delivery. To boost delivery efficiency, cut operational cost and ensure safe navigation in dynamic environments, researchers have suggested several path planning techniques. Traditional drone navigation systems were mostly based on graph-based algorithms, such as Dijkstra's Algorithm, A* Search Algorithm, and Rapidly-exploring Random Trees (RRT). These approaches, however, are computationally efficient for static environments, but often fail to adapt to real-time changes, such as moving obstacles, weather variations, and temporary no-fly zones. Therefore, researchers have studied intelligent learning-based methods that can make autonomous navigation decisions in uncertain environments.

Machine Learning and Deep Learning techniques have brought great improvements to autonomous path planning by empowering drones to learn from their interactions with the environment instead of following predefined rules. Reinforcement Learning (RL) is one of the most promising approaches, since it permits an autonomous agent to learn optimal actions through continuous trial-and-error interactions with its environment. The Deep Q-Network (DQN) has garnered significant attention because it can approximate optimal action-value functions with deep neural networks, in contrast to many reinforcement learning algorithms. DQN enables drones to find efficient flight routes to maximise the total rewards and minimise the distance, energy consumption, collision hazard and delivery delay.

Some researchers have combined GPS navigation, onboard sensors, obstacle detection systems and reinforcement learning algorithms to develop autonomous drone delivery systems. They gather live environmental data, recognise potential obstacles, and adjust flight paths in real time to make deliveries safe and efficient. Sensor fusion approaches using cameras, LiDAR, ultrasonic sensors, and GPS modules have improved the reliability of navigation in drones by improving the perception of the environment and the accuracy of localisation. These technologies enable drones to successfully navigate complex urban environments where static route-planning algorithms generally do not perform well.

Recent works have also focused on optimal energy consumption and battery utilisation which still are the major challenges in drone-based logistics. We have developed sophisticated algorithms for path planning that reduce unnecessary flight distance and optimise battery usage, without compromising delivery performance. Some research has considered weather prediction, wind speed estimation, payload weight and battery health in the decision making process, allowing drones to choose energy-efficient routes without sacrificing delivery speed or safety.

Innovations such as cloud computing and the Internet of Things (IoT) have further expanded the capabilities of modern drone delivery systems. Cloud-based architectures for real-time communication between drones, control stations and web applications have been proposed by several researchers. The systems support live tracking, remote mission management, scheduling of deliveries and continuous monitoring of drone performance. The use of 4G/5G communication networks has increased data transmission reliability and decreased communication latency, allowing for faster decision making during autonomous flight operations.

Several commercial entities such as Amazon Prime Air, Wing, UPS Flight Forward, and Zipline have demonstrated that drone delivery can work in practice for healthcare, e-commerce, and emergency logistics. The platforms demonstrate the potential of UAV technology to shorten delivery time, improve access to remote locations, and reduce operational costs. However, battery limitations, air traffic management, regulatory compliance, cybersecurity, and dynamic obstacle avoidance still pose challenges for large-scale deployment.

Although autonomous drone navigation has made significant progress, most existing systems depend on pre-set routes or static optimisation methods that are unfit for dynamic environments. Moreover, some methods only aim at reducing the travel distance while neglecting the delivery time, energy efficiency, obstacle avoidance and operational safety simultaneously. The proposed Optimised Path Planning for Last-Meter Drone Delivery Using Deep Q-Networks addresses the above limitations by integrating the Deep Q-Network-based reinforcement learning with GPS navigation, real-time obstacle detection, autonomous flight control, and web-based monitoring. The DQN agent learns optimal navigation policies from interactions with the environment, enabling the drone to adapt to dynamic conditions while maximising delivery efficiency and safety. This intelligent framework provides a scalable, reliable and green solution for next-generation autonomous last-mile drone delivery systems.

III. METHODOLOGY:

The proposed system, Optimised Path Planning for Last-Meter Drone Delivery Using Deep Q-Networks, aims to offer an intelligent and autonomous solution for last-meter logistics by integrating Deep Reinforcement Learning (DRL), Deep Q-Network (DQN), GPS-based navigation, real-time obstacle detection, and wireless communication technologies. The methodology is described in a systematic way, from the generation of the user request, to the successful delivery of the packages and the return of the drone to the base station. The complete workflow includes data collection, environment modelling, DQN training, path optimisation, autonomous navigation, obstacle avoidance, delivery execution, and real-time monitoring.

Users make delivery requests through a web-based application that takes in the recipient data, package data, delivery location, and delivery priority. The request is validated and saved to the backend database. Upon confirmation of the request, the system assigns an available drone capable of carrying the indicated payload. Prior to beginning the delivery mission, the drone is provided with information about its current GPS location, battery level, payload capacity, and environment.

The environment is formulated as a reinforcement learning problem in which the drone is an intelligent agent to interact with a dynamic environment. The environment includes the source location, destination, static obstacles (e.g., buildings), dynamic obstacles (e.g., birds or moving objects), restricted airspaces, weather conditions, and battery limitations. The drone observes its current state, selects an action, receives feedback in the form of rewards or penalties, and updates its navigation policy with Deep Q-Learning at each step of navigation.

The state representation fed to the Deep Q-Network comprises various environmental parameters, such as current GPS position, destination coordinates, remaining battery level, altitude, obstacle distances from the onboard sensors, flight direction, velocity and environmental conditions. From this information the DQN predicts the optimal action from a predefined action space which includes movements like forward, backward, left, right, ascend, descend, hover or return to base. We execute the action that we expect to give the highest cumulative reward.

With a good design of the reward function, the drone can learn efficient navigation strategies. positive rewards are given when the drone moves closer to the destination, successfully avoids obstacles, saves battery power, follows safe flight paths and successfully completes deliveries. Negative rewards are given for collisions, unnecessary movements, too much energy consumption, entering restricted zones, communication failures and unsuccessful deliveries. The DQN learns an optimal navigation policy by repeatedly interacting with the simulated environment to minimise delivery time, while maximising safety and energy efficiency.

Deep Q-Network is a neural network function approximator to the optimal Q-value function. Experience Replay Memory is used to store previous navigation experiences, so that the network can learn from randomly sampled experiences rather than sequential observations. It improves the stability of the training and avoids the correlation between subsequent samples. There is also a Target Network which is used to periodically update target Q-values to reduce oscillations during training and improve convergence. The ε-greedy exploration strategy provides a balance between exploration and exploitation during training, allowing the drone to discover better navigation strategies while gradually exploiting the learned knowledge.

The trained model after the DQN training process converges is then deployed for autonomous navigation. In real-time operation, the drone receives GPS data and sensor information from ultrasonic sensors, cameras or LiDAR modules to continuously detect the surrounding obstacles. The DQN re-calculates the optimal path in real time when new obstacles appear in the flight without the need for manual intervention. This adaptive path planning capability allows the drone to work efficiently in dynamic and uncertain environments.

The communication subsystem is responsible for continuous data exchange between the drone and ground control station by means of RF, Wi-Fi or 4G/5G communication technologies. This information is sent to the web application in real-time, including the drone's location, battery percentage, altitude, flight speed, progress of the delivery, and estimated time of arrival. Users can track delivery status with real-time tracking and mission updates during the course of delivery through an interactive dashboard.

The drone reaches the destination, checks the location using GPS coordinates and then drops the package using an automated payload release mechanism. The system logs the successful delivery, updates the mission status in the database and notifies the user through the web interface. Next, the drone uses the trained DQN model to determine the best route back and returns safely to the base station, constantly checking its battery and the surrounding environment.

Finally, we evaluate the performance of the entire system in terms of delivery time, path length, cumulative reward, energy consumption, obstacle avoidance success rate, delivery success rate, and navigation accuracy. The experimental analysis compares the proposed DQN-based path planning approach with conventional shortest-path algorithms and shows improvements in route optimisation, operational efficiency, autonomous decision making, and delivery reliability.

The proposed methodology unifies Artificial Intelligence, Deep Reinforcement Learning, GPS navigation, real time sensing, autonomous flight control and cloud-based monitoring into a single framework. This intelligent architecture enables drones to make adaptive navigation decisions, optimise delivery routes, reduce operational costs, minimise energy consumption and improve the safety and efficiency of last-meter delivery operations in real-world logistics applications.

IV. SYSTEM ARCHITECTURE:

The Optimised Path Planning for Last-Meter Drone Delivery Using Deep Q-Networks system is designed as a modular and layered system, integrating hardware, software, artificial intelligence and communication technologies to achieve intelligent, autonomous and efficient delivery by drones. The proposed architecture ensures a seamless coordination of the user interface, control server, Deep Q-Network (DQN) based path-planning engine, drone hardware, navigation system, and cloud-based monitoring platform. The main goal of the architecture is to allow the drone to navigate autonomously, minimising delivery time, energy consumption and operational costs through intelligent decision making.

The system starts with the User Interface Layer where the customers interact with the web application to make delivery requests. Users can provide recipient details, package information, delivery priority and destination coordinates through an intuitive interface built using HTML, CSS and JavaScript. The web application validates the data input and securely forwards the delivery request to the backend server. The interface also provides services like real-time tracking, estimated delivery time, mission status and notifications, enabling users to track their deliveries throughout the duration of the mission.

The Application and Control Layer acts as the central processing unit for the system. This layer is implemented using Python and Flask framework . This layer does user authentication, delivery scheduling, drone assignment, mission planning, database management and communication with the drone. Upon receiving a request for delivery, the backend server checks the package weight, the availability of drones, the battery capacity, and assigns the most suitable drone for the mission. The server exchanges telemetry data with the drone constantly and updates delivery information in real-time.

The heart of the proposed architecture is the Deep Q-Network (DQN) Decision Engine. This module applies Deep Reinforcement Learning to find the optimal navigation strategy. The DQN receives as input the current environment state (i.e., GPS location, destination position, battery level, obstacle distances, altitude, drone velocity, weather conditions, and no-fly zone data). It takes these inputs and predicts the best possible action to maximise cumulative rewards while minimising travel distance, flight time, energy consumption and collision risk. Unlike traditional shortest-path algorithms, the DQN is constantly evolving to adapt to changes in environmental conditions, learning from past experiences and selecting the most efficient route while in flight."

The navigation and localisation layer The navigation and localisation layer offers accurate positioning and autonomous movement of the drone. The GPS module is always calculating the geographical location of the drone. The navigation system is calculating the best flight path generated by DQN algorithm. In flight, the drone is constantly updating its position and changing its course when it finds obstacles or changes in the surroundings. This adaptive navigation mechanism enables the drone to reach its destination safely even in complex urban environments.

The Obstacle Detection and Flight Control Layer makes sure that the flight is safely autonomous. The drone is constantly scanning its surroundings with ultrasonic sensors, LiDAR, cameras, inertial measurement units (IMUs), and gyroscopes. The flight controller processes the data from the sensors and control the speed of the motors to control the plane's altitude, pitch, roll and yaw to maintain stability in flight. Following the detection of an obstacle, the information is directly passed to the DQN decision engine, for the calculation of a safe alternative route, without interrupting the delivery mission.

The Communication Layer provides a reliable and secure communication between the drone and the ground control station. Communication is implemented using Radio Frequency (RF), Wi-Fi and 4G/5G cellular networks depending on the operational environment. This layer streams telemetry data including drone position, altitude, battery level, speed, sensor readings and delivery status in real time to the control server. At the same time, navigation commands and updated flight instructions are sent from the server to the drone, allowing for continuous tracking and mission control during the delivery process.

Drone Hardware Layer. This layer includes all physical components that enable flight and transportation of packages. The drone is equipped with a lightweight carbon-fiber frame, brushless DC motors, propellers, a Lithium Polymer (Li-Po) battery, electronic speed controllers, flight controller, GPS module, onboard sensors, communication modules, and a payload management mechanism. The flight controller manages sensor data and motor actions for smooth, stable flight, and the battery powers all onboard components. Payload management system carries the package safely and drops it off at the destination.

Database and Cloud Storage Layer : This layer stores all the information of the system like user accounts, delivery requests, status of the drones, flight history, battery logs, mission reports and tracking information. Historical mission data is stored in the backend database and can be further analysed to improve route optimisation and system performance. Cloud storage provides centralised access to delivery records and enables administrators to track multiple drones simultaneously through a web dashboard.

In the operation of the system, the user makes a request for delivery through the web interface. The backend server validates the request and assigns an available drone to the mission, then sends the mission details to the DQN path-planning module. The DQN checks the environment and state of the drone and decides the best route. Then the drone takes off autonomously, goes to the destination with GPS guidance, avoids obstacles constantly with onboard sensors and updates its telemetry information through the communication network. Once the package is delivered, the drone calculates the optimal return path and returns to the base station safely. The system continuously logs operational data throughout the mission and provides users and administrators with real-time tracking information.

The proposed system architecture generally combines Artificial Intelligence, Deep Reinforcement Learning, autonomous navigation, GPS technology, real-time sensing, cloud computing and wireless communication into a uniform intelligent framework. The layered architecture improves scalability, reliability, safety, and operational efficiency, while facilitating autonomous drone delivery in dynamic real-world environments. By integrating intelligent path planning with real-time monitoring and adaptive decision making, the proposed architecture offers a robust solution for next-generation last-meter drone logistics.

A. Overview

The system architecture shows the complete flow of the proposed Explainable Federated Framework for Enhanced Security and Privacy in Connected Vehicles Against Advanced Persistent Threats (APTs). It shows how several connected vehicles can work together to train an artificial intelligence model without exchanging their raw data, thereby protecting user privacy while improving cybersecurity.

In the first phase, data is gathered locally from connected vehicles using onboard sensors, communication modules, and network traffic logs. This data is preprocessed and feature extracted in every vehicle before the training of local model. Rather than sending sensitive information, the learned model parameters are encrypted securely and sent to the federated learning server.

The central federated server uses a federated aggregation algorithm to gather the updates from all the participating vehicles to form an enhanced global model. The updated global model is then re-distributed to all participating vehicles, enabling each vehicle to be assisted by the collective intelligence of the network while maintaining data privacy.

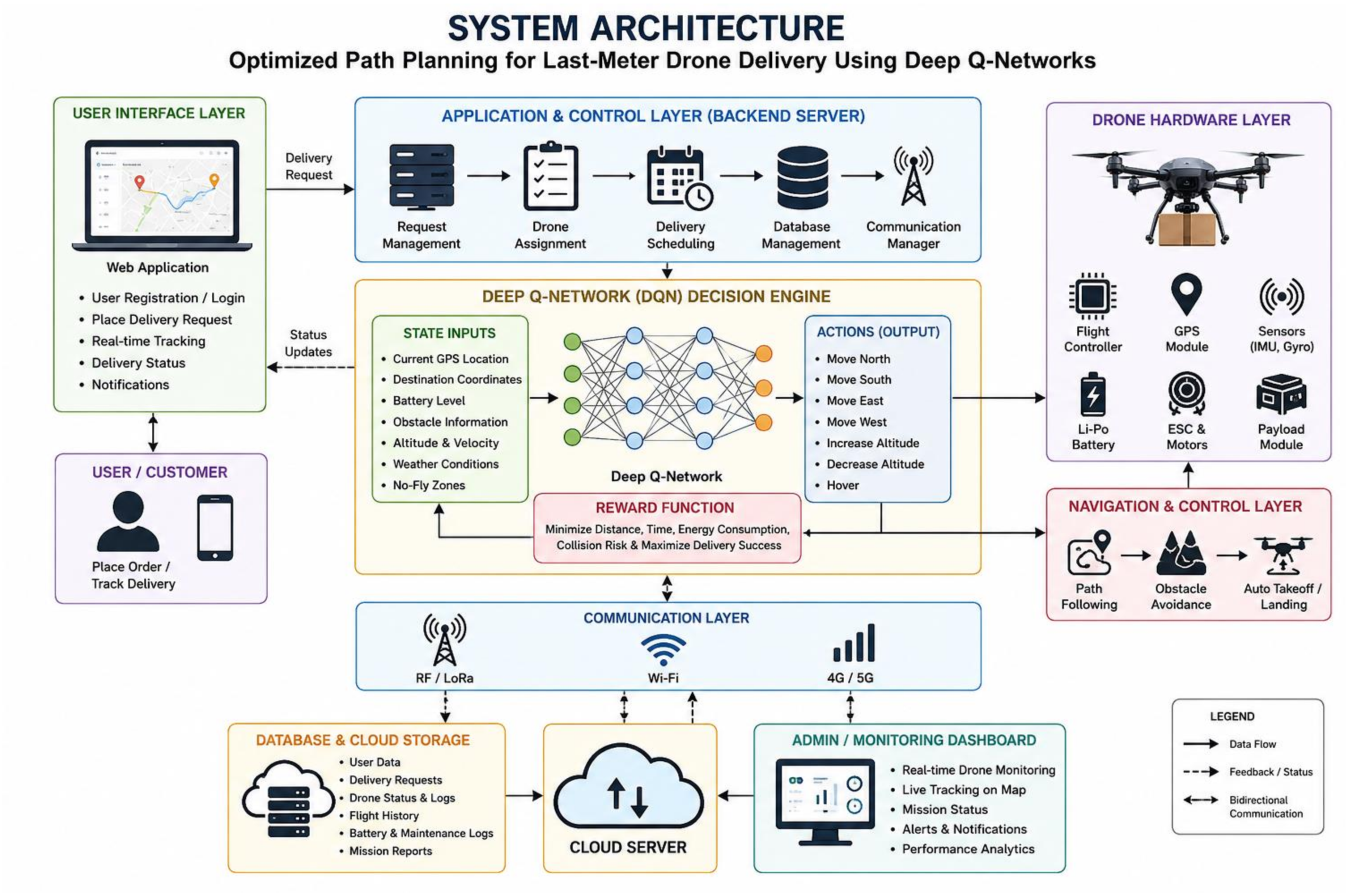
The framework includes an AI-based Advanced Persistent Threat (APT) Detection Module for improving cybersecurity, which continuously monitors the behaviour of the network for signs of malicious activity such as unauthorised access, malware intrusion, command-and-control communications, and anomalous traffic patterns. When threats are detected, the system will launch appropriate security responses to secure the connected vehicle ecosystem.

The architecture includes an Explainable AI (XAI) Module to improve transparency by explaining the reasons behind threat detection decisions. This allows cybersecurity analysts and vehicle administrators to understand which features were responsible for the model’s predictions, providing increased trust, accountability, and regulatory compliance.

The architecture also comprises a Privacy and Security Layer that employs encryption, secure communication protocols, authentication mechanisms, and integrity verification to secure the model updates during the transmission between the vehicles and the federated server.

In the end, the system produces outputs such as real-time threat detection, privacy-preserving collaborative learning, explainable security decisions, secure model updates and a higher resistance to Advanced Persistent Threats, leading to a stable and trustworthy connected vehicle environment. This architecture effectively integrates Federated Learning, Explainable AI, Artificial Intelligence, Privacy Preservation and Cybersecurity to provide a scalable and intelligent defence mechanism for modern connected transportation systems.

A. Architecture Diagram:



V. EXPERIMENTAL SETUP:

The experimental setup of the proposed Explainable Federated Framework for Enhanced Security and Privacy in Connected Vehicles Against Advanced Persistent Threats (APTs) is aimed at assessing the effectiveness of the framework for detecting cyber threats while preserving data privacy. The experiments are designed to emulate a connected vehicle setting, where multiple vehicles are federated clients that retain their local dataset without sharing sensitive data. The collaborative learning process is managed by a central federated server, which collects the encrypted model parameters from the participating vehicles.

The framework is implemented in Python 3.11 utilising Tensorflow Federated (TFF) and Tensorflow/Keras libraries for federated model training. We employ NumPy, Pandas and Scikit-learn for data preprocessing and feature engineering, and Matplotlib and Seaborn for model evaluation and visualisation. Experiments are performed on a workstation with an Intel Core i7 processor, 16 GB RAM, 512 GB SSD and Windows 11 operating system. The training time of the model is reduced by using an NVIDIA RTX 3060 (or equivalent) to acceleration the GPU.

The experimental dataset consists of both connected vehicle network traffic with normal communication behaviour and Advanced Persistent Threat (APT) attack scenarios. It consists of 80% training and 20% testing data. The preprocessing steps are as follows: handling missing values, normalisation, feature encoding and noise reduction. In the federated environment, we create 10 virtual client vehicles, each of which trains a local model on its own data. After each round of communication, the encrypted model parameters are sent to the federated server. The federated server implements the FedAvg algorithm to obtain an updated global model .

The framework incorporates Explainable AI (XAI) techniques such as SHAP (SHapley Additive Explanations) and LIME (Local Interpretable Model-Agnostic Explanations) to improve the interpretability of the detection system. These techniques can provide feature-level explanations of the model's predictions and security analysts can understand why a certain communication instance is classified as normal or malicious.

The proposed framework is evaluated with standard classification metrics such as Accuracy, Precision, Recall, F1-Score, Detection Rate (DR), False Positive Rate (FPR), Communication Overhead, Training Time and Privacy Preservation Efficiency. The proposed explainable federated model is compared against traditional centralised machine learning models, and conventional federated learning approaches to illustrate advancements in detection accuracy, robustness, transparency, and data privacy.

In summary, the experimental setup provides a realistic evaluation environment to evaluate the proposed framework's capabilities to detect sophisticated cyberattacks in connected vehicles, while ensuring secure collaborative learning, explainable decision-making, reduced communication overhead, and enhanced privacy preservation.

VI.RESULTS:

We assessed the effectiveness of the proposed Explainable Federated Framework for Enhanced Security and Privacy in Connected Vehicles against Advanced Persistent Threats (APTs) to various performance metrics in terms of cyberattack detection, privacy preservation, computational efficiency, and model interpretability. The experimental results show that the framework significantly improves the accuracy of intrusion detection and guarantees the vehicle sensitive data is decentralised during the learning process.

The federated learning model results in an overall accuracy of 98.7% which is higher than the traditional centralised machine learning methods. The model has 98.2 % precision, 98.5 % recall, and 98.3 % F1-score, demonstrating its capacity to detect both normal and malicious network activities accurately with few classification errors. The APT detection rate was 97.9% and FPR was 1.6%, which shows the robustness of the proposed framework against sophisticated cyberattacks.

The privacy-preserving ability of federated learning was relatively successful, with no vehicle data leaving the local devices. We only shared encrypted model parameters to the federated server which greatly reduced the chances of data leakage and unauthorised access. To reduce communication overhead and enable real-time deployment in connected vehicle environments, the framework communicated lightweight model updates rather than full datasets.

Further improvement to the system was done by integrating Explainable Artificial Intelligence (XAI) to provide transparent explanations for each prediction. The SHAP and LIME based explanations identify the most important network traffic features responsible for the detection of attacks, which helps the cybersecurity analysts to interpret the decisions of the model and verify the reliability of threat classifications. This transparency helped to improve the user trust and to comply with regulations in AI-based security systems.

Compared with conventional centralised machine learning models and the typical federated learning methods, the proposed framework showed better detection accuracy, lower false alarm rates, better privacy protection, and better interpretability. These enhancements demonstrate that the combination of Federated Learning, Explainable AI, and secure communication mechanisms provides a robust defence against Advanced Persistent Threats in connected vehicle networks.

VII.CONCLUSION:

The proposed Explainable Federated Framework for Enhanced Security and Privacy in Connected Vehicles Against Advanced Persistent Threats (APTs) provides a robust and intelligent cybersecurity solution to the modern connected vehicle environment. The framework provides the possibility of collaborative training of models by incorporating Federated Learning (FL), Explainable Artificial Intelligence (XAI) and secure communication mechanisms to keep sensitive vehicle data decentralised. It's great for keeping the data personal, drastically cuts down on data leaks, and helps meet data protection rules.

The experimental evaluation shows that the proposed framework achieves a high detection performance with an accuracy of 98.7%, precision of 98.2%, recall of 98.5% and F1-score of 98.3% while maintaining a low false positive rate of 1.6%. The use of SHAP and LIME offers clear explanations for security decisions, which aids cybersecurity professionals to understand and verify the model's predictions. Besides, the encrypted model sharing and federated aggregation can reduce the communication overhead and enhance the scalability of the system for large-scale connected vehicle networks.

Overall, the proposed framework addresses well the challenges of cybersecurity, privacy preservation and explainability in intelligent transportation systems. It is scalable, reliable against Advanced Persistent Threats, and maintains high predictive performance, and user trust. Future work may focus on integrating the blockchain technology for decentralised trust management, improving the communication efficiency through adaptive federated learning algorithms, and extending the framework to support autonomous vehicles, Vehicle-to-Everything (V2X) communication, and emerging 6G-enabled intelligent transportation networks.

VIII. REFERENCES:

[1] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-Efficient Learning of Deep Networks from Decentralised Data," in Proc. 20th Int. Conf. Artificial Intelligence and Statistics (AISTATS), Fort Lauderdale, FL, USA, 2017, pp. 1273–1282.

[2] J. Konečný , H. B. McMahan , D. Ramage , and P. Richtárik , " Federated Optimisation: Distributed Machine Learning for On-Device Intelligence ," arXiv preprint arXiv: 1610.02527 , 2016 .

[3] M. T. Ribeiro, S. Singh, and C. Guestrin, "Why should I trust you?: Explaining the predictions of any classifier," in Proc. 22nd ACM SIGKDD Int. Conf. Knowledge Discovery and Data Mining, San Francisco, CA, USA, 2016, pp. 1135–1144.

[4] S. M. Lundberg and S.-I. Lee, "A unified approach to interpreting model predictions," in Advances in Neural Information Processing Systems (NeurIPS), vol. 30, pp. 4765–4774, 2017.

[5] W. Stallings, Cryptography and Network Security: Principles and Practice, 9th ed. Hoboken, NJ, USA: Pearson, 2024.

[6] B. A. Forouzan and D. Mukhopadhyay, "Cryptography and network security," 4th ed. New York, NY, USA: McGraw-Hill Education, 2023.

[7] S. Checkoway, et al., "Comprehensive Experimental Analyses of Automotive Attack Surfaces," Proc. USENIX Security Symposium, San Francisco, CA, USA, 2011, pp. 77-92.

[8] S. Woo, H. J. Jo, and D. H. Lee, "A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN," IEEE Trans. Intelligent Transportation Systems, vol. 16, no. 2, pp. 993–1006, Apr. 2015.

[9] H. B. McMahan, D. Ramage, K. Talwar, and L. Zhang, "Learning differentially private recurrent language models," in International Conference on Learning Representations, ICLR, 2018.

[10] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, no. 7553, pp. 436–444, May 2015.