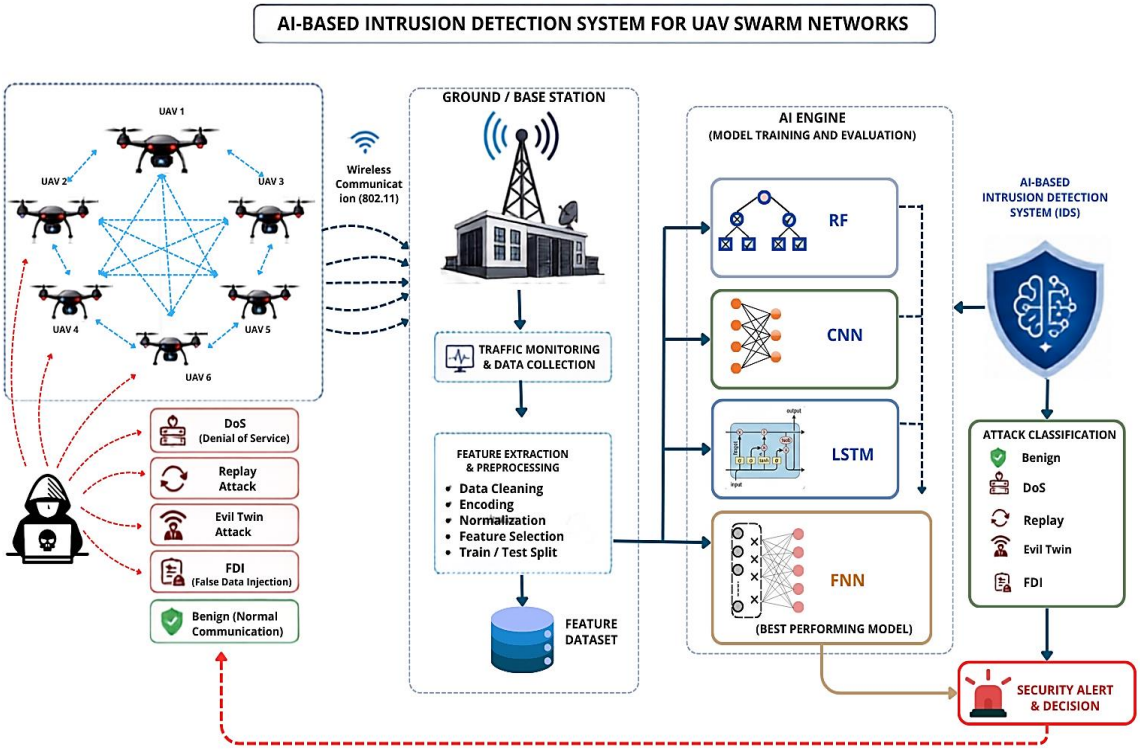
Final Year Design Project Showcase
Batch-2022
Year 2026

Department: Telecommunications Engineering Programme: **Telecommunications Engineering**	
1	**Project Title** Design and Evaluation of AI-Driven Intrusion Detection System for UAV Swarm Networks
2	**Project Idea** Unmanned Aerial Vehicle (UAV) swarm networks are increasingly used in surveillance, disaster response, military operations, border monitoring, and smart city applications. However, their decentralized wireless communication makes them highly vulnerable to cyberattacks such as Denial of Service (DoS), Replay, Evil Twin, and False Data Injection (FDI). This project proposes an Artificial Intelligence (AI)-driven Intrusion Detection System (IDS) capable of identifying multiple cyberattacks in UAV swarm networks. A real cyber-physical UAV dataset was preprocessed using data cleaning, normalization, categorical encoding, feature engineering, and SMOTE for class balancing. Four AI models Random Forest, Feedforward Neural Network (FNN), One-Dimensional Convolutional Neural Network (1D-CNN), and Long Short-Term Memory (LSTM) were developed and evaluated to compare their classification performance, computational efficiency, and deployment suitability for resource-constrained UAV platforms.
3	**Process** The project followed a systematic AI development methodology consisting of the following steps: • Selection of a real cyber-physical UAV swarm dataset containing benign traffic and multiple attack categories. • Data preprocessing, including removal of corrupted and duplicate records, encoding of categorical features, normalization of numerical values, and balancing the dataset using SMOTE. • Feature engineering to identify the most informative features for intrusion detection. • Splitting the dataset into training and testing sets. • Training four AI models: Random Forest, 1D-CNN, Feedforward Neural Network (FNN), and Long Short-Term Memory (LSTM). • Evaluating each model using Accuracy, Precision, Recall, F1-Score, and Confusion Matrix. • Comparing all models based on classification performance, model size, inference speed, computational efficiency, and suitability for deployment on resource-constrained UAV platforms.

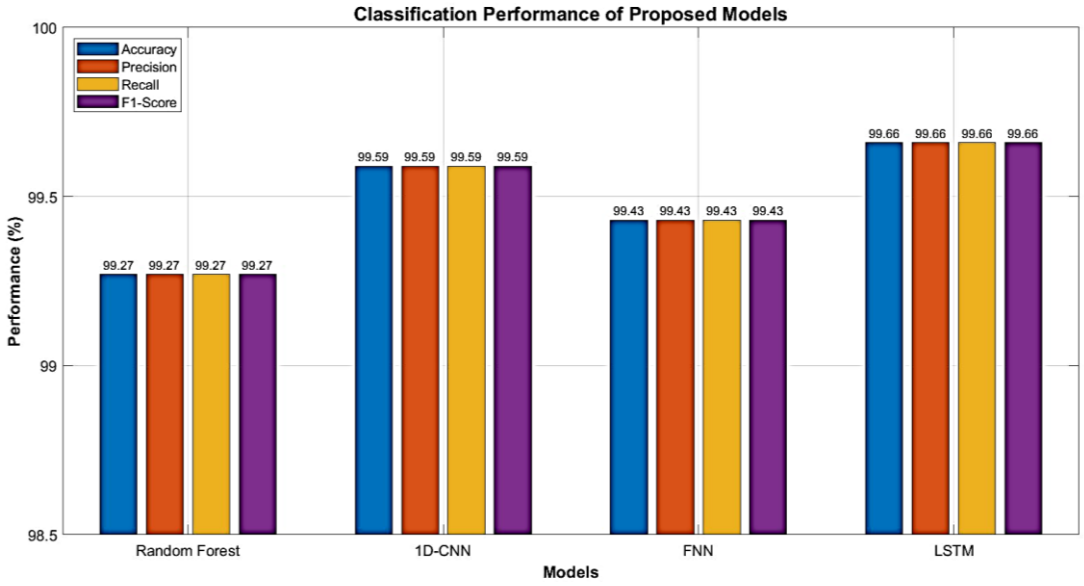
4	**Outcome** The developed AI-based Intrusion Detection System successfully detected multiple cyberattacks in UAV swarm networks with excellent classification performance. Among the evaluated models, the LSTM classifier achieved the highest test accuracy of 99.66%, followed by the 1D-CNN (99.59%), Feedforward Neural Network (99.43%), and Random Forest (99.27%). All four models demonstrated excellent classification performance. The comparative evaluation identified LSTM as the highest-performing model in terms of accuracy, while FNN offered the smallest model size (19.77 KB), making both suitable for different UAV deployment requirements. The project confirms that AI-based intrusion detection significantly enhances the cybersecurity, reliability, and operational safety of UAV swarm communication networks.
5	**Evidence (Theoretical Basis)** The project is supported by an extensive literature review on Artificial Intelligence, Machine Learning, Deep Learning, UAV swarm communication, and Intrusion Detection Systems. Experimental validation was carried out using a real cyber-physical UAV dataset containing more than 54,000 labeled communication packets. The dataset included benign traffic as well as DoS, Replay, Evil Twin, and False Data Injection attacks. After preprocessing and feature engineering, four different AI models were trained and evaluated using standard performance metrics. The developed system was benchmarked by comparing model accuracy, precision, recall, F1-score, lightweight deployment characteristics, and inference performance to identify the most suitable solution for practical UAV swarm security.
6	**Competitive Advantage or Unique Selling Proposition** This project presents an AI-driven Intrusion Detection System (IDS) for UAV swarm communication networks using a real cyber-physical dataset. Four machine learning and deep learning models were evaluated under identical conditions to identify solutions that provide high detection accuracy while remaining suitable for deployment on resource-constrained UAV platforms. The proposed framework improves UAV communication security and offers a scalable solution for future autonomous aerial systems.
a	**Attainment of any SDG** (e.g. How it is achieved and why it is necessary for the region) The proposed system contributes to the following Sustainable Development Goals (SDGs): **SDG 9 – Industry, Innovation and Infrastructure** by improving the cybersecurity and reliability of intelligent UAV communication systems used in smart infrastructure, surveillance, logistics, and industrial automation. **SDG 11 – Sustainable Cities and Communities** by enabling secure UAV applications for disaster response, public safety, environmental monitoring, and smart city services.
b	**Any Environmental Aspect** (e.g. carbon reduction, energy-efficient, etc.) The proposed AI models are computationally efficient, enabling energy-conscious deployment on UAV platforms. Early intrusion detection also reduces mission failures and improves overall utilization of UAV resources.
c	**Cost Reduction of Existing Product**

	Traditional UAV security solutions often rely on expensive hardware or specialized security equipment. The proposed software-based AI intrusion detection system can be integrated into existing UAV platforms without additional hardware modifications, reducing implementation and maintenance costs.
d	**Process Improvement which Leads to Superior Product or Cost Reduction, Efficiency Improvement of the Whole Process** (e.g. What is the issue is current process and what improvement you suggests) Conventional intrusion detection systems mainly rely on predefined rules and signatures, making them ineffective against evolving cyber threats. The proposed AI-driven IDS automatically learns communication patterns from real UAV traffic and detects previously unseen attacks with high accuracy. This improves detection speed, reduces false alarms, enhances network reliability, and supports real-time security monitoring.
e	**Expanding of Market share** (e.g. how it expand and what is the problem with the current market) The proposed system increases confidence in UAV security, encouraging wider adoption across industries such as defense, smart cities, precision agriculture, disaster management, logistics, infrastructure inspection, and environmental monitoring.
f	**Capture New Market** (e.g. Niche market or unaddressed segment) The project enables secure deployment of autonomous UAV swarms in safety-critical applications including military surveillance, emergency response, border security, industrial inspection, and intelligent transportation systems where strong cybersecurity is essential.
g	**Any Other Aspect** Unlike many previous studies based on simulated datasets, this project evaluates four AI models using a real cyber-physical UAV dataset under a common experimental framework. This provides a reliable comparison for selecting suitable intrusion detection models for practical UAV deployment.
7	**Target Market** (Industries, Groups, Individuals, Families, Students, etc) Please provide some detail about the end-user of the product, process, or service The proposed AI-based Intrusion Detection System is intended for organizations that require secure UAV communication systems, including: • Defense and security organizations operating UAV swarms. • Telecommunications and wireless communication industries. • Smart city infrastructure developers. • Disaster management and emergency response agencies. • Border surveillance and law enforcement organizations. • UAV manufacturers and autonomous drone solution providers. • Cybersecurity companies developing AI-based network protection solutions.

	• Universities and research institutions working on UAV security and Artificial Intelligence.	
8	**Team Members** (Names along with email address)	Arshia Naveed (TC-22020) arshia4530254@cloud.neduet.edu.pk Anees-Ur-Rehman (TC-22036) anees-ur-rehman4503066@cloud.neduet.edu.pk Malaika Ghazanfar (TC-22046) malaikaghazanfar25@gmail.com Shaista Hassan (TC-22049) shaistahassan228@gmail.com
10	**Supervisor Name** (along with email address)	Dr. Hira Mariam hiramariam@cloud.neduet.edu.pk
11	**Video (If any)**	N/A
12	 ***Pictures (to be pasted below)*** *Comprehensive diagram showing the structure of the system*

Model	Overall Accuracy	Weighted Precision	Weighted Recall	Weighted F1-Score
Random Forest	99.27%	0.9927	0.9927	0.9927
1D-CNN	99.59%	0.9959	0.9959	0.9959
FNN	99.43%	0.9943	0.9943	0.9943
LSTM	99.66%	0.9966	0.9966	0.9966

Consolidated Classification Performance of All Proposed Models



Model	Parameters	Model Size	Inference Latency
Random Forest	214,000	21.35 MB	0.0096 ms/sample
1D-CNN	34,437	0.131 MB	0.1 ms/sample
FNN	5,061	19.77 KB	0.0118 ms/sample
LSTM	60,101	0.229 MB	0.0712 ms/sample

Consolidated Lightweight Deployment Metrics of All Proposed Models