Graphic Era deemed to be University DEHRADUN

# PROJECT AND TEAM INFORMATION

## Project Title

(Try to choose a catchy title. Max 20 words).

*Transparent and privacy derived Xai and FL based Framework for the intrusion detection and explanation of IDS*

## Student/Team Information

| | |
|---|---|
| *Team Name:*<br>*Team #* | *Catch the Rainbow*<br>*CYBER-IV-T066* |
| **Team member 1 (Team Lead)** | *Omar Bin Nasir - 230111620*<br>*omarbinnasir24@gmail.com*<br>  |

| | |
|---|---|
| **Team member 2**<br>*(Last Name, name: student ID: email, picture):* | *Pitamber Mehra - 23021779*<br>*pitambermehra85@gmail.com*<br>  |
| **Team member 3**<br>*(Last Name, name: student ID: email, picture):* | *Sayyam Thapliyal – 230213691*<br>*sayyamthapliyal2005@gmail.com*<br>  |
| **Team member 4**<br>*(Last Name, name: student ID: email, picture):* | *PRIYANSHU PANDEY – 230211548*<br>*priyanshupandey9112@gmail.com*<br>  |

# PROJECT PROGRESS DESCRIPTION (35 pts)

## Project Abstract (2 pts)

(Brief restatement of your project's main goal. Max 300 words).

The goal of this project is to develop a transparent and privacy-preserving Intrusion Detection System (IDS) that leverages Explainable AI and Federated Learning. This system aims to detect both known and novel cyber threats effectively while ensuring data privacy and providing interpretable results to enhance trust among security analysts

## Updated Project Approach and Architecture (2 pts)

(Describe your current approach, including system design, communication protocols, libraries used, etc. Max 300 words).

Our approach involves using the NSL-KDD dataset for training various machine learning models, including Logistic Regression, Decision Trees, and K-Nearest Neighbors, alongside existing models like Random Forest and SVM. We will implement a federated learning framework to maintain data privacy and utilize explainable AI techniques (e.g., SHAP, LIME) to provide insights into model decisions.

## Tasks Completed (7 pts)

(Describe the main tasks that have been assigned and already completed. Max 250 words).

| Task Completed | Team Member |
|---|---|
| Literature review and dataset finalization<br>Data preprocessing and exploratory analysis<br>Implementation of baseline models<br>Implementation of XAI on models | Sayyam Thapliyal ,Priyanshu Pandey<br>Pitamber Mehra<br>Omar Bin Nasir<br>Omar Bin Nasir |

## Challenges/Roadblocks (7 pts)

(Describe the challenges that you have faced or are facing so far and how you plan to solve them. Max 300 words).

We faced challenges with high false positive rates in initial model evaluations and difficulties in integrating federated learning components. To address these, we are refining our model parameters and seeking guidance on the implementation of federated learning techniques. Regular team meetings will help ensure alignment on these issues.

## Tasks Pending (7 pts)

(Describe the main tasks that you still need to complete. Max 250 words).

| Task Pending | Team Member (to complete the task) |
|---|---|
| Implementing FL | Sayyam Thapliyal |

## Project Outcome/Deliverables (2 pts)

(Describe what are the key outcomes / deliverables of the project. Max 200 words).

Key deliverables include a fully functional IDS capable of real-time threat detection, source code for all implemented models, performance reports with evaluation metrics, and comprehensive documentation detailing our approach and results.

## Progress Overview (2 pts)

(Summarize how much of the project is done, what's behind schedule, what's ahead of schedule. Max 200 words.)

Currently, about 70% of the project is complete. Model implementation is on schedule, while documentation is slightly behind due to the need for additional testing. We expect to catch up in the coming weeks as we finalize model evaluations.

## Codebase Information (2 pts)

(Repository link, branch, and information about important commits.)

Repository link: https://github.com/OmarBinNasir/IDS
Branch: main
Important commits include the initial model implementations and integration of XAI techniques.

## Testing and Validation Status (2 pts)

(Provide information about any tests conducted)

| Test Type | Status (Pass/Fail) | Notes |
|---|---|---|
| Data Preproessing<br>Model Train<br>Model Accuracy<br>XAI explaination | Pass<br>Pass<br>Pass<br>Pass | |

## Deliverables Progress (2 pts)

(Summarize the current status of all key project deliverables mentioned earlier. Indicate whether each deliverable is completed, in progress, or pending.)

All key deliverables are currently in progress, with model implementations completed and documentation being finalized. Expected completion within the next two weeks.