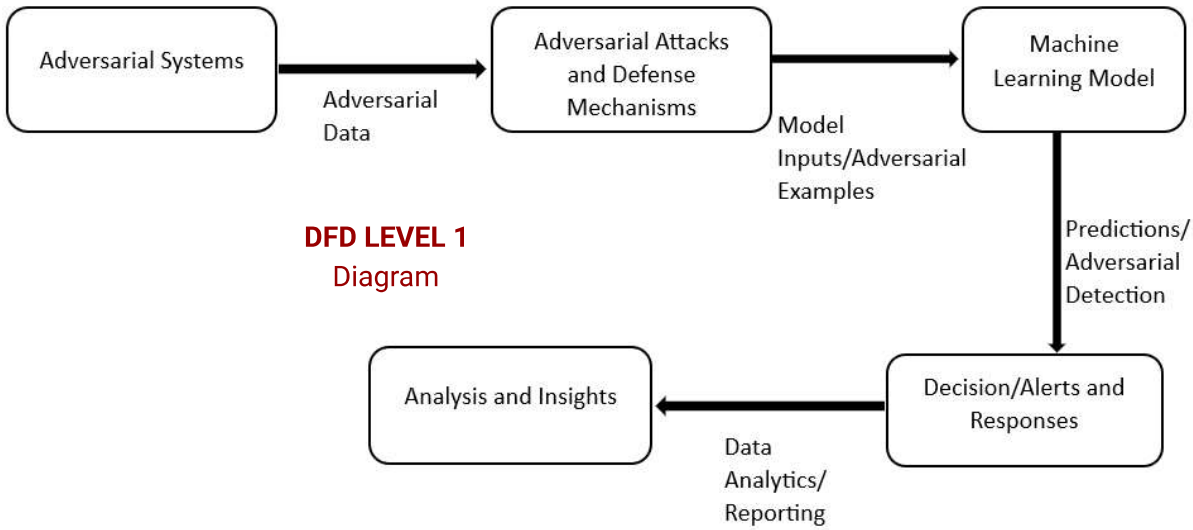
Project Design Phase-II
Data Flow Diagram

Date	**29th October 2023**
Team ID	**TEAM 3.1**
Project Name	**Adversarial Attacks and Defenses**

Data Flow Diagram:



DFD LEVEL 1
Diagram

- The Adversarial System represents the core system responsible for managing adversarial attacks and defenses.
- Adversarial Attacks and Defense Mechanisms include processes for both launching and defending against attacks. They may include anomaly detection, adversarial training, and other strategies.
- Machine Learning Model(s) receive inputs, make predictions, and may employ defense mechanisms, including adversarial detection and recognition.
- The Decision/Alerts and Responses component responds to model predictions, adversarial attack alerts, and can trigger various actions or responses.
- Analysis and Insights can involve in-depth analytics, reporting, and the extraction of actionable insights from the data.

User Stories -

Example - Garbage classification model

User Type	Functional Requirement (Epic)	User Story Number	User Story / Task	Acceptance criteria	Priority	Release
Waste management companies	Project setup & Infrastructure	USN-1	Set up the development environment with the required tools and frameworks to start the garbage classification project.	successfully configured with all necessary tools and frameworks	High	Sprint 1
Municipalities and Local Governments	development environment	USN-2	Gather a diverse dataset of images containing different types of garbage (plastic, paper, glass, organic) for training the deep learning model.	Gathered a diverse dataset of images depicting various types of garbage	High	Sprint 1
Households and Individuals	Data collection	USN-3	Preprocess the collected dataset by resizing images, normalizing pixel values, and splitting it into training and validation sets.	preprocessed the dataset	High	Sprint 2
Researchers and Academics	data preprocessing	USN-4	Explore and evaluate different deep learning architectures (e.g., CNNs) to select the most suitable model for garbage classification.	we could explore various DL models	High	Sprint 2
Non-Governmental Organizations (NGOs)	model development	USN-5	train the selected deep learning model using the preprocessed dataset and monitor its performance on the validation set.	we could do validation	High	Sprint 3
Educational Institutions	Training	USN-6	implement data augmentation techniques (e.g., rotation, flipping) to improve the model's robustness and accuracy.	we could do testing	medium	Sprint 3
	model deployment & Integration	USN-7	deploy the trained deep learning model as an API or web service to make it accessible for garbage classification. integrate the model's API into a user-friendly web interface for users to upload images and receive garbage classification results.	we could check the scalability	medium	Sprint 4
	Testing & quality assurance	USN-8	conduct thorough testing of the model and web interface to identify and report any issues or bugs. fine-tune the model hyperparameters and optimize its performance based on user feedback and testing results.	we could create web application	medium	Sprint 5