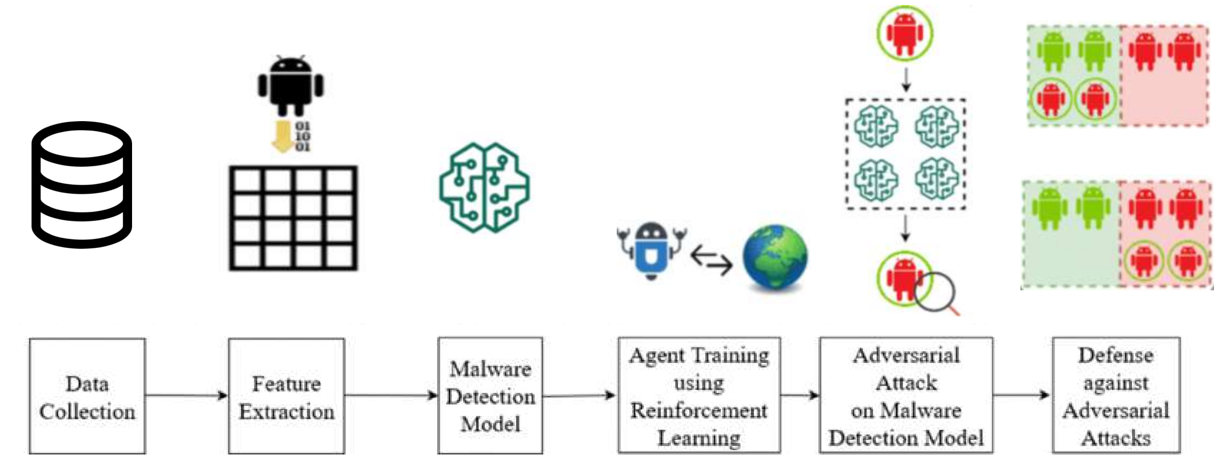
Project Design Phase-I
Solution Architecture

Date	**31st October 2023**
Team ID	**TEAM 3.1**
Project Name	**Adversarial Attacks and Defenses**

Solution Architecture:

- The solution architecture for addressing adversarial attacks and defenses in machine learning comprises a robust foundation of machine learning models and defense mechanisms.
- We start with gathering data of discovered attack algorithms used for adversarial attacks, faulty image identifications and breaches.
- Next classifying the machine learning algorithms to train our framework(API)
- Our solution, i.e, our framework will work as a Malware detection tool to address adversarial attacks and detect image identification breaches.

Solution Architecture Diagram:


01
10
01
Data Collection
Feature Extraction
Malware Detection Model
Agent Training using Reinforcement Learning
Adversarial Attack on Malware Detection Model
Defense against Adversarial Attacks

(Data training) (Decompiling & forming feature vector) (Classification Algorithms) (Agent Environment Interaction) (Modification Attack) (Before and after Defense)