**SOLUTION ARCHITECTURE**

Date: 24/10/2023

Team ID: 2.10

Project name: Malware Detection and Classification

Team members: Sohan, Shaz, Atharva, Pratheek

A solution architecture for malware detection and classification involves collecting and preprocessing malware data, employing machine learning models, feature extraction, real-time analysis, and integrating threat intelligence. It should also incorporate feedback loops, reporting, quarantining, and ensure compliance with privacy regulations and robust security measures. The architecture should be scalable, continuously updated, and adaptable to evolving threats.

To train a multi-classification model and a malware-detection model, we first prepare the training and test datasets which contain different malware types such as flooder, adware, spyware, etc., as well as benign objects. We then convert the portable executables (PE) objects into greyscale images.

* Data Collection and Preprocessing: Collect and preprocess malware data from various sources, preparing it for analysis.
* Machine Learning Models: Employ supervised or unsupervised machine learning models for malware detection and classification.
* Real-Time Analysis and Feedback: Implement real-time analysis, integrate threat intelligence, and establish feedback loops for continuous learning and improvement.
* Security and Compliance: Ensure robust security measures, privacy compliance, scalability, and adaptability to evolving threats in the architecture.

**SOLUTION ARCHITECTURE DIAGRAM**

