

Project Design Phase-I
Solution Architecture

Date	30 October 2023
Team ID	Team – 587578 (2.12)
Project Name	MALWARE DETECTION AND CLASSIFICATION
Maximum Marks	4 Marks

Team Members:

Naladala Navya

Sanisetty Hema Sagar

Kurra Naveen Abhiram

Vishnubhatla V L Sruta Keerthi

Solution Architecture:

Solution architecture is a complex process – with many sub-processes – that bridges the gap between business problems and technology solutions. Its goals are to:

- Building an efficient detection system requires gathering samples of both malicious and benign software from several sources and properly classifying them with regard to the different categories of malware.
- To improve model performance, it is crucial to extract pertinent features from malware samples and carry out feature selection/extraction.
- Malware detection is based on the creation and training of machine learning models, which can combine deep learning and conventional ML models.
- Reliable results are guaranteed when cross-validation is used in conjunction with proper assessment measures to assess model performance.
- For the detection system to be available, a suitable deployment platform—such as on-premises servers or cloud services—must be chosen.
- It is crucial to have strong security measures in place to guard against adversarial assaults on the models and private information.
- System dependability depends on continuously checking the deployed models for performance deterioration or concept drift and setting up warning mechanisms for quick response.

- Ensuring smooth operation under changing loads is achieved by applying load balancing and designing the architecture to manage varying traffic volumes.
- Usability and functionality are increased by creating an intuitive user interface, offering choices for uploading files or URLs for scanning, and including APIs for integration.
- Legal and operational integrity depend on a number of factors, including making sure that all applicable rules and regulations are followed, keeping accurate records, and educating analysts and administrators.

Example - Solution Architecture Diagram:

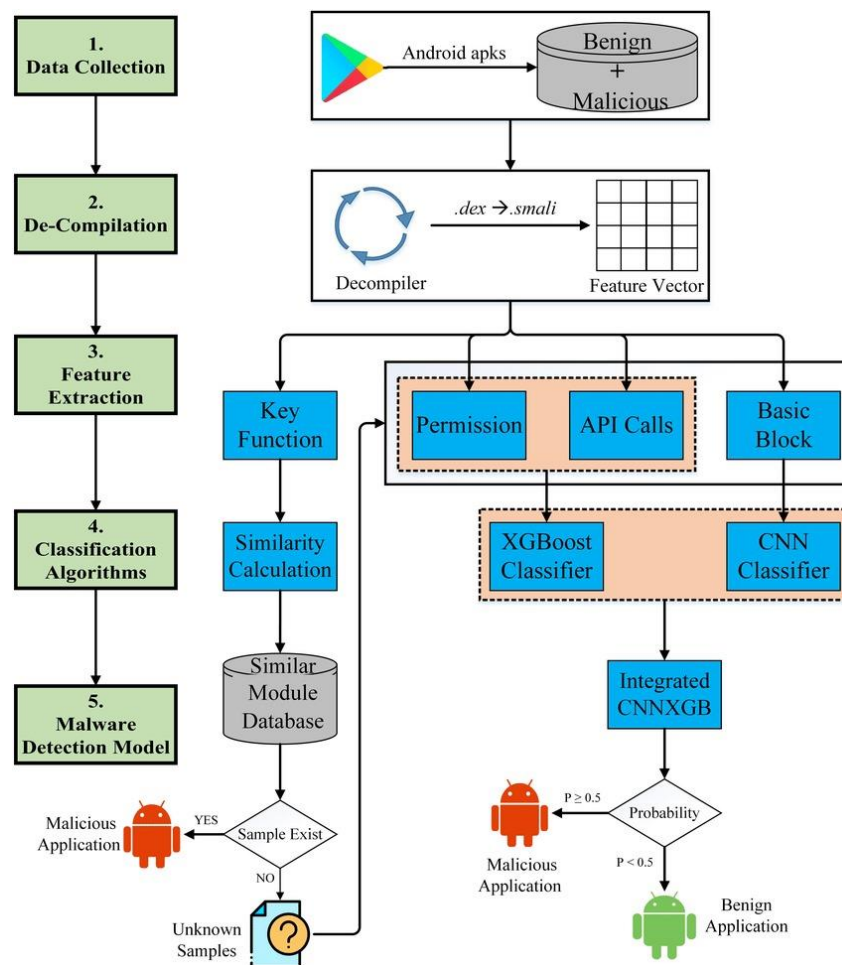


Figure 1: Architecture and data flow of the Malware Detection and Classification

Reference: https://www.researchgate.net/figure/System-Architecture-of-the-Android-malware-detection-using-hierarchical_fig1_349162676