Project Design Phase-I
Solution Architecture

Date	25 October 2023
Team ID	2.1
Project Name	MALWARE DETECTION AND CLASSIFICATION
Maximum Marks	4 Marks

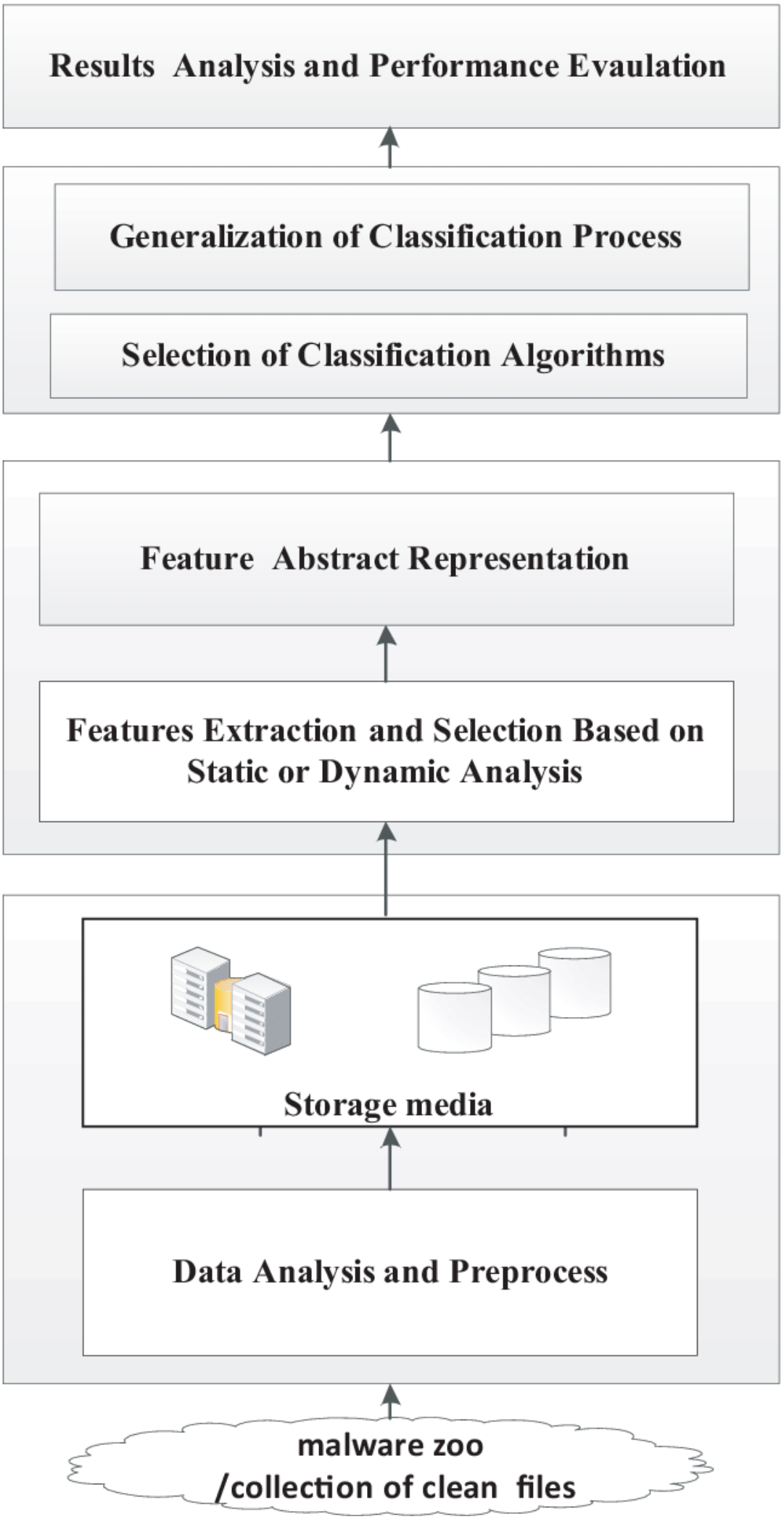
Solution Architecture:

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

#) Behavioral analysis examines the malware specimen's interactions with its environment: the file system, the registry (if on Windows), the network, as well as other processes and OS components. As the malware investigator notices interesting behavioral characteristics, he modifies the laboratory environment to evoke new characteristics.

#) **Code analysis** reverse-engineers the malicious program to understand the code that implements the specimen's behavior. When looking at compiled programs, this process involves using a disassembler, a debugger and, perhaps, a decompiler to examine the program's low-level assembly or byte-code instructions

#) **Memory analysis** examines memory of the infected system to extract artifacts relevant to the malicious program. In the context of reverse-engineering malware, memory analysis can help identify malicious code that is trying to hide itself (i.e., rootkits), can clarify the program's run-time dependencies, and can explain how the specimen was used on the victim's system.


Results Analysis and Performance Evaulation
Generalization of Classification Process
Selection of Classification Algorithms
Feature Abstract Representation
Features Extraction and Selection Based on Static or Dynamic Analysis
Storage media
Data Analysis and Preprocess
malware zoo
/collection of clean files

In above diagram we explain Architecture of Our Malware Detection and Classification System.

Solution Architecture Diagram