Project Design Phase-I
Solution Architecture

Date	12 September 2023
Team ID	2.3
Project Name	Malware Detection And Classification
Maximum Marks	4 Marks

Solution Architecture:

The architecture for Malware Detection and Classification comprises several key components. It begins with data intake, where a diverse dataset of malware samples is collected and continuously updated to account for new threats. Model testing ensures the effectiveness of the Convolutional Neural Network (CNN) model in identifying and classifying malware. Subsequently, model training takes place, where the CNN is fed with labeled data to learn the distinguishing features of various malware types. Data transformation involves preprocessing raw malware data, making it suitable for analysis. A test dataset is used to assess the model's accuracy and generalization. Finally, the model is deployed in real-time, allowing for immediate malware detection and classification. This architecture provides a dynamic and adaptive solution for combating evolving malware threats while ensuring the system's accuracy and reliability in safeguarding against cyberattacks.

- Data intake
- Model testing
- Model training
- Test dataset
- Data transformation
- Model deployment

Solution Architecture Diagram: