Aakash R
CB.SC.P2CYS23011

How machine learning is utilized for malware detection:

Machine learning can be used for malware detection in Android by training models to recognize patterns and features indicative of malicious behaviour. Here's a short explanation of the process:

1. **Data Collection**: Gather a large dataset of Android applications, including both benign and malicious samples.
2. **Feature Extraction**: Extract relevant features from the apps, such as permissions, API calls, network traffic patterns, and code structure.
3. **Model Training**: Use the extracted features to train machine learning models, such as decision trees, support vector machines, or neural networks. The model learns to distinguish between benign and malicious apps based on the provided features.
4. **Model Evaluation**: Validate the model using a separate dataset to ensure its accuracy, precision, recall, and overall effectiveness in detecting malware.
5. **Deployment**: Integrate the trained model into a malware detection system that can analyze new apps in real-time, flagging those that exhibit suspicious behavior for further review or automatic action.

By continuously updating the model with new data and refining its features, machine learning can provide an effective and adaptive solution for identifying and mitigating malware threats on Android devices.

The below screenshot specifies the website from which datasets can be obtained from.