The uploaded paper outlines a variety of **machine learning (ML)** and **deep learning (DL)** models specifically used for malware detection. Below is a summary of the models mentioned in the paper:

**Machine Learning (ML) Models**

1. **Support Vector Machines (SVM):**
   * Used for classifying malware images (e.g., grayscale, RGB, HSV).
   * Example: Chauhan et al. (2022) achieved 96% accuracy using SVM on malware images.
2. **Random Forest (RF):**
   * Applied for analyzing features like system logs, API calls, and opcode sequences.
3. **K-Nearest Neighbors (KNN):**
   * Used for basic classification tasks in malware detection.
4. **Decision Trees (DT):**
   * Utilized to analyze static and dynamic malware features.
5. **Gradient Boosting Methods:**
   * Models like XGBoost are referenced for boosting accuracy in malware classification.

**Deep Learning (DL) Models**

1. **Convolutional Neural Networks (CNN):**
   * Widely applied for **malware image classification**.
   * Examples include:
     + **ResNet**, **Inception-V3/V4**, **EfficientNet (B0 to B7)**, **DenseNet**, and **Xception**.
     + These models process grayscale and RGB malware images.
   * Accuracy:
     + Inception-V4 achieved 95.98% accuracy on the Malimg dataset.
2. **Recurrent Neural Networks (RNN):**
   * Combined with CNNs for analyzing **sequential data** like API calls and opcode sequences.
3. **Capsule Networks (CapsNet):**
   * An advanced architecture for malware image classification.
   * Example: Achieved 96.6% F-Score on the Malimg dataset.
4. **Generative Adversarial Networks (GANs):**
   * Used to generate adversarial examples for improving model robustness and malware detection.
5. **Hybrid Models:**
   * **Multi-modal Deep Learning:** Combines grayscale images, byte histograms, and entropy features.
   * **Deep Multi-task Learning:** Handles malware detection across multiple operating systems (Windows, Linux, Android, etc.).

**Natural Language Processing (NLP)**

1. **Sequence-to-Sequence Models:**
   * Used for malware detection with API calls, logs, and opcode sequences.
   * Often incorporates **attention mechanisms** for better performance.
2. **Text Embedding Models:**
   * Includes Bag of Words (BoW), TF-IDF, and advanced embeddings like Word2Vec for analyzing textual features of malware.

**Transfer Learning Models**

1. **Pre-trained Models on ImageNet:**
   * Examples: VGG16, Inception-V4, EfficientNet, Xception, and ResNeXt.
   * Fine-tuned for malware image datasets (e.g., Malimg, BIG2015).

**Explainable AI (XAI)**

1. Techniques like LIME (Local Interpretable Model-agnostic Explanations) and DeepLIFT (Deep Learning Important Features) are used to interpret model decisions in malware detection tasks.

**Adversarial Defense Models**

1. Models designed to counter **adversarial attacks**:
   * Conditional GANs (Conv-GANs).
   * Semi-black-box frameworks like "Malfox" for generating robust adversarial examples.

This paper extensively reviews and evaluates these models in terms of accuracy and robustness for malware detection across multiple datasets and operating systems.