International Journal On Engineering Technology and Sciences – IJETS
ISSN (P):2349-3968, ISSN (O): 2349-3976 Volume XI - Issue IV, April – 2024

CONSTRUCTION WORKERS SAFETY PRODUCTS DETECTION USING YOLOV7

[1]Manoj kumar.C, [2]Ajith.J, [3]Abishek.R, [4]Parthasarathi, [5]Mr.Syed Mohamed Ali. M
[1,2,3,4]Student, [5]Assistant Professor
Department of Information Technology
Loyola Institute of Technology and Science, Nager coil, Tamilnadu

Abstract : Using multiple linear regression models for malware detection on Android might not be the most suitable approach. Linear regression is typically used for predicting continuous variables, whereas malware detection is a classification problem where the goal is to categorize instances into different classes (e.g., malware or benign)For malware detection, you would typically use classification algorithms, such as logistic regression, decision trees, random forests, support vector machines (SVM), or deep learning methods like convolutional neural networks (CNNs) or recurrent neural networks (RNNs).

IndexTerms Detecting Android malware using multiple linear regression models based on classifiers involves several step. Data Collection Gather a dataset containing features extracted from Android applications. These features may include permissions requested, API calls made, app size, code complexity metrics, etc. Each sample in the dataset should be labeled as either malware or benign.. Feature Engineering: Preprocess the dataset by cleaning, normalizing, and selecting relevant features. Feature engineering may also involve dimensionality reduction techniques like PCA (Principal Component Analysis) to reduce the number of features while preserving information. **Model Training**: Split the dataset into training and testing sets. Train multiple classification models such

INTRODUCTION

In recent years, the proliferation of Android devices has led to an increase in the development of mobile applications. However, this rapid growth has also attracted malicious actors who exploit vulnerabilities within these applications to distribute malware. Detecting and mitigating Android malware has become a critical concern for users, developers, and security experts alike.

Traditional approaches to Android malware detection often rely on classification algorithms such as decision trees, support vector machines (SVM), or deep learning methods like convolutional neural networks (CNNs). However, in this study, we propose a novel approach that leverages multiple linear regression models as the basis for classification.

The motivation behind using multiple linear regression lies in its simplicity and interpretability. By representing the relationship between various features extracted from Android applications and their corresponding malware labels, we aim to uncover patterns that distinguish malicious apps from benign ones.

This paper presents a comprehensive framework for detecting Android malware using multiple linear regression models based on classifiers. We begin by discussing the dataset used for training and evaluation, followed by an explanation of feature extraction and engineering techniques. Subsequently, we delve into the construction of multiple linear regression models and their integration with classification algorithms.

II.PROPOSED SYSTEM:

Our proposed system for detecting Android malware utilizes multiple linear regression models as the foundation for classification. The system comprises several key components and steps:

1. Data Collection and Preprocessing:

- Gather a diverse dataset of Android applications, including both malware and benign samples.
- Extract relevant features from each application, such as permissions requested, API calls made, file system interactions, and other behavioral characteristics.
- Preprocess the data by cleaning, normalizing, and transforming features as necessary to prepare it for model training.

2. Feature Engineering:

- Conduct feature selection and dimensionality reduction to identify the most informative features while reducing computational complexity.

- Explore techniques such as correlation analysis, mutual information, or recursive feature elimination to identify the most discriminative features for malware detection.

3. Model Training:

- Construct multiple linear regression models, each focusing on different subsets of features or feature combinations.

- Utilize techniques such as forward selection, backward elimination, or stepwise regression to iteratively build regression models with the most predictive power.

- Incorporate regularization techniques like Lasso or Ridge regression to prevent overfitting and improve model generalization.

4. Classification Integration:

- Integrate the output of the linear regression models with traditional classification algorithms to make final predictions.

- Use thresholds or decision rules to convert regression outputs into binary malware/non-malware predictions.

- Explore ensemble methods such as bagging or boosting to combine predictions from multiple regression-based classifiers for improved performance.

5. Model Evaluation:

- Evaluate the performance of the proposed system using standard metrics such as accuracy, precision, recall, F1-score, and receiver operating characteristic (ROC) curves.

- Conduct cross-validation to assess the robustness of the models and ensure they generalize well to unseen data.

- Compare the performance of the proposed system against baseline classifiers and state-of-the-art malware detection approaches to validate its effectiveness.

6. Deployment and Integration:

- Integrate the trained models into a real-time Android malware detection system or security suite.

- Develop APIs or libraries to facilitate easy integration with existing Android security frameworks or antivirus solutions.

- Continuously monitor and update the models to adapt to emerging malware threats and maintain high detection accuracy.

By following this systematic approach, our proposed system aims to provide an effective and scalable solution for detecting Android malware using multiple linear regression models as the basis for classification.

REFERENCES

1. Arp, Daniel, et al. "DREBIN: Effective and Explainable Detection of Android Malware in Your Pocket." Proceedings of the 21st Annual Network and Distributed System Security Symposium (NDSS). 2014.
2. Sufatrio, Mohammad, et al. "Detecting Android Malware Using Static Analysis Based on Principal Component Analysis and K-Nearest Neighbor." International Journal of Computer Applications 121.13 (2015): 12-18.
3. Zhou, Yajin, et al. "Hey, You, Get Off of My Market: Detecting Malicious Apps in Official and Alternative Android Markets." Proceedings of the 19th Annual Network and Distributed System Security Symposium (NDSS). 2012.
4. Kantchelian, Alex, et al. "Detecting Android Malware Using Longitudinal Data." Proceedings of the 5th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices (SPSM). 2015.
5. Xu, Weixiong, et al. "Mining Behavioral Semantics for Detecting Android Malware." IEEE Transactions on Information Forensics and Security 10.5 (2015): 1059-1072.