RANSOMWARE DETECTION AND RECOVERY PLANNING

Harshith Martha, Preet Patel, Sai Sri Harsha Kumbam, Ramya Jyotsna Neelakantrao, Jaswanth Ram Nagabhyrava
University of Maryland, Baltimore County (UMBC)

Abstract

In this digital age detecting ransomware is very crucial than ever our project addresses these needs by applying datamining and machine learning algorithms to accurately detect ransomware files by analyzing a diverse set of data we developed a model that detects ransomware threats contributing to the enhancement to of cybersecurity with an accuracy of 92%

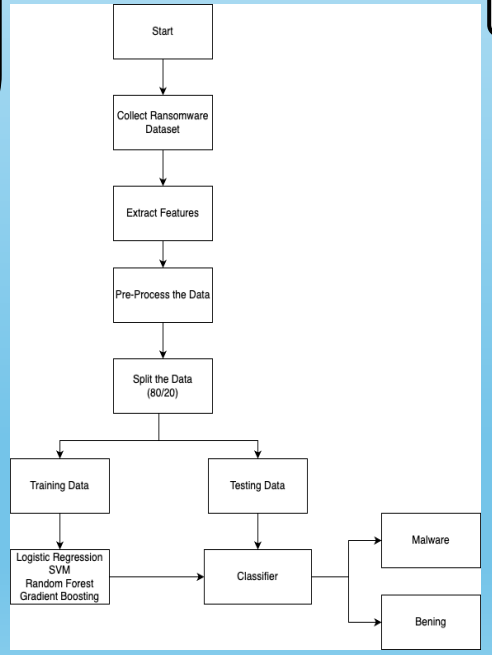
Related Work

The application of machine learning, Random Forests, in our project was influenced by Siddiqui et al.'s (2008) groundbreaking work on static binary feature extraction for ransomware detection. This method was further developed by Mohaisen and Alrawi (2015), who used machine learning to examine characteristics like file size and DLL imports. Their research helped us with feature engineering and the application of SVM and other models to improve detection accuracy.

Data

The dataset utilized in our project is publically available on kaagle it composed of approx. 62000 instances and 18 attributes this extensive dataset encompasses of both malware and benign files providing a diverse foundation for implementing ML models

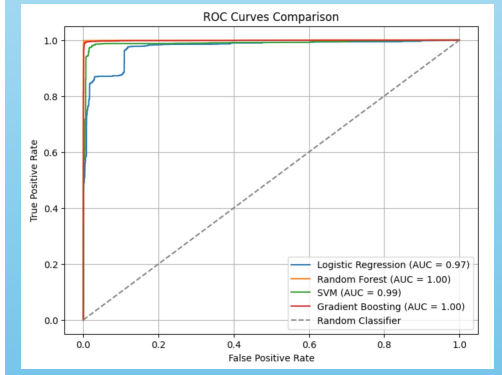
Methodology

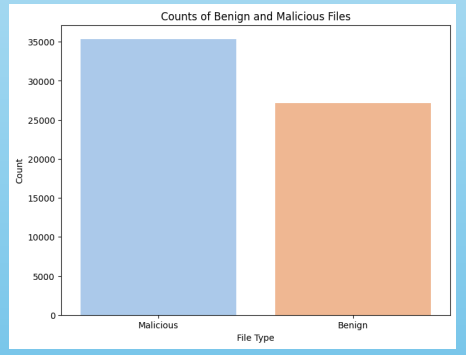


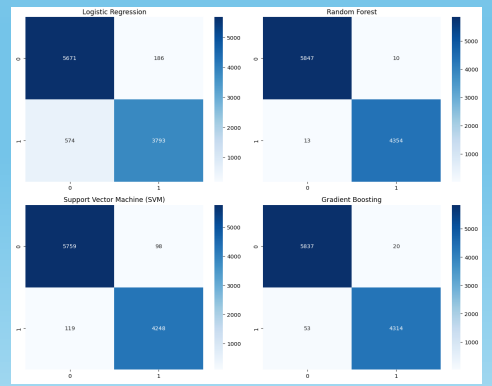
Implementation:

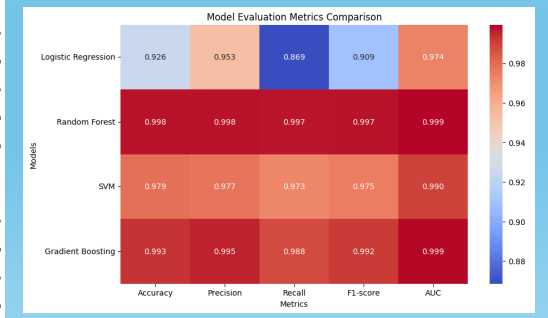
Step1: Data Cleaning
Step 2: Feature Selection & Normalization
Step-3: Data Exploration
Step-4: Data Splitting
Step-5: Model Training
Step-6: Testing

Results









Conclusion

The Ransomware based malware and benign classification using machine learning using different modeling techniques. In conclusion present study offers important information about how machine learning are used to detect. Ransomware the outcome provides starting point and more study in the field.

Future Work

In the subsequent research, we plan to integrate advanced data mining techniques for more detailed analysis and classification also in future works other machine learning algorithms can be implemented and also new records cane be taken from real world and see that the model does not over fit on the test data