WINDOWS THREAT HUNTING

Nagkichan MOUSTAFA IMPRAM
Supervisor: Assist. Prof. Dr. Şaban SAHMOUD

ABSTRACT

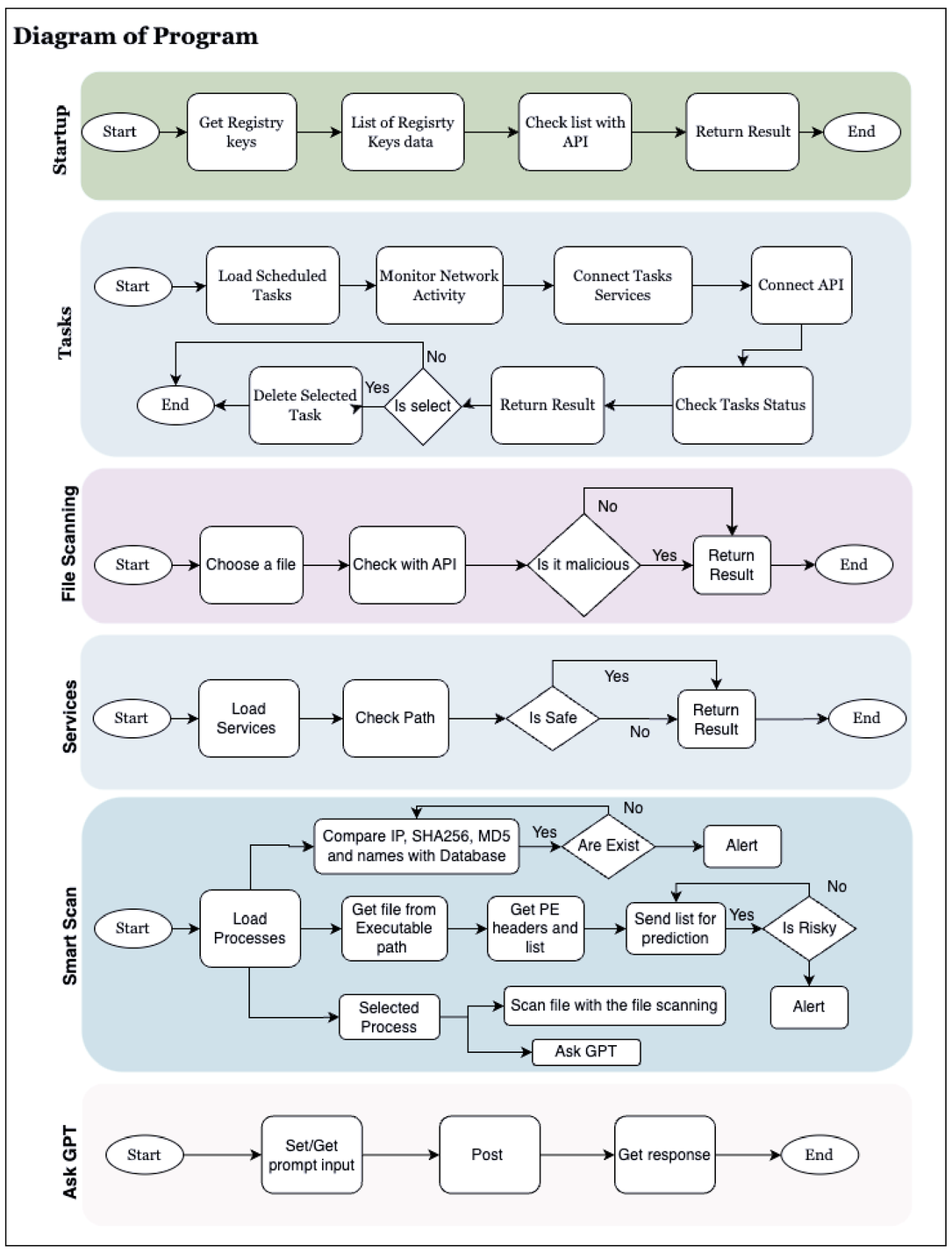
An innovative system has been developed to detect malware residing on Windows operating systems. The project aims to enhance computer security and provide effective protection against cyber threats.

INTRODUCTION

The Virus Detection System project aims to help users keep their computers secure and reduce digital security concerns. Malicious software that is installed unnoticed and continues to run in the background can slow down systems or gain unauthorized access to personal data. Therefore, tracking downloaded files and their processes to minimize the risk of infection and inform users about potential threats is of great importance.

FLOW DIAGRAM

The general flow diagram of the project developed for the Virus Detection System consists of six different sections.



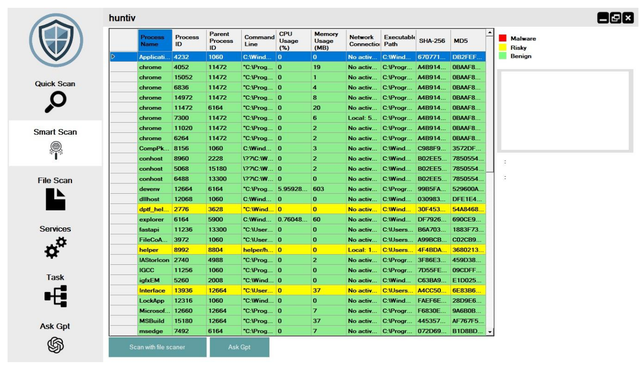
METHODOLOGY

Multiple methods are used in this project to improve virüs detection techniques.

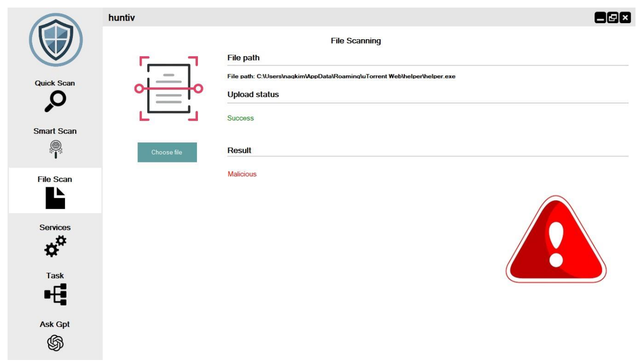
- A dataset has been created by monitoring system logs, recording the behavior and actions of over 30 viruses. As a result, common patterns have been identified, forming the dataset.
- Machine learning is used for virus detection.
- API usage: Four different APIs have been integrated to conduct broader and more comprehensive detections across various areas.

RESULTS

The machine learning model used has achieved highly accurate results.



API usage in the project provides both automatic and on-demand detailed analysis options.



CONCLUSION

The dataset used is an alternative source of data. Although it provides highly accurate results, it has not been sufficiently tested. To ensure safer usage, the number of tested files needs to be increased.