UE20CS390A – Capstone Project Phase – 1

+ Project Title : Detection and Prevention of Covert Channel
+ Project ID : PW23_SVM_01
+ Project Guide : Dr. Sapna V M
+ Project Team : 153_184_193_290

Problem Statement

Is your data safe?

Are the existing tools enough?

How to counter the data exfiltration through hidden channels?

Abstract

Covert Channels pose a serious threat to the privacy by acting as a means for data exfiltration by malware.

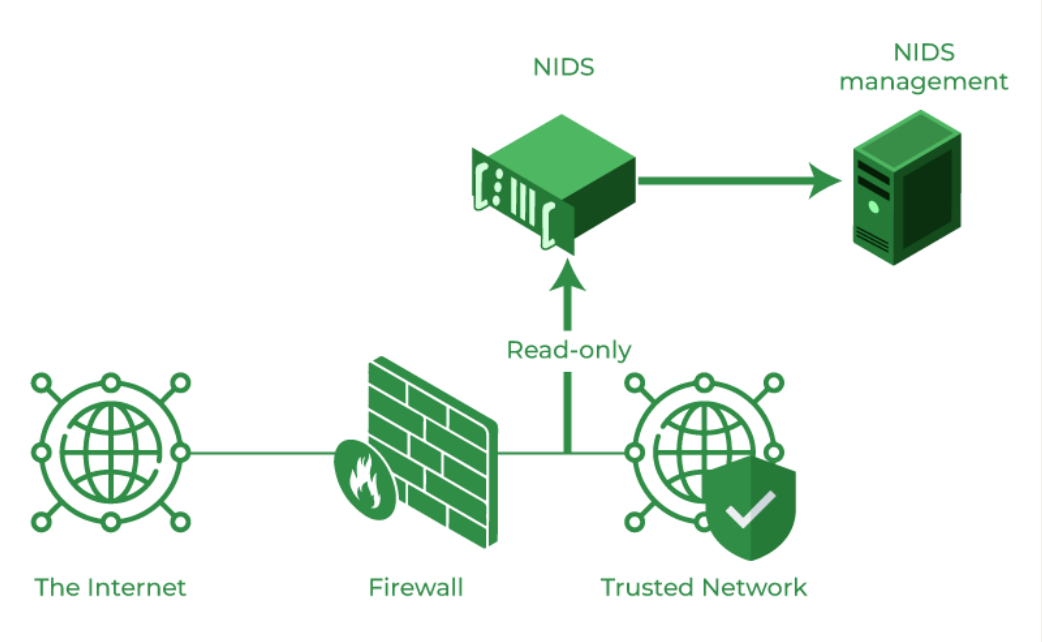
Even though data channels have higher throughput, timing channels are relatively difficult to detect since they operate over prolonged period of time and the amount of data per network packet is very low.

The proposed solution filters the packets based on a superficial detection techniques and also employs machine learning approach to detect the covert channel accurately

Suggestion from previous reviews

+ Demonstration of Covert channel
+ Dataset generation tool
+ Visualization of packet presence

How feasible is the solution?



ADDS MINIMUM OVERHEAD

HIGHLY ACCURATE

ADDITIONAL SECURITY

PROTECTS THE DATA

Takeaways from Literature survey

- Use of ***BCCStego*** like took for packet summarization
- Use of technique used by ***CCgen*** for generation of dataset by inserting covert channels into real-world traffics.
- Use of classification algorithm like ***SVM*** might yield better results
- Techniques to ***filter*** the packets beforehand by using common characteristics of covert channels like the type of data, frequency of packets etc.

Design Approach

FILTERING

DETECTION

PREVENTION

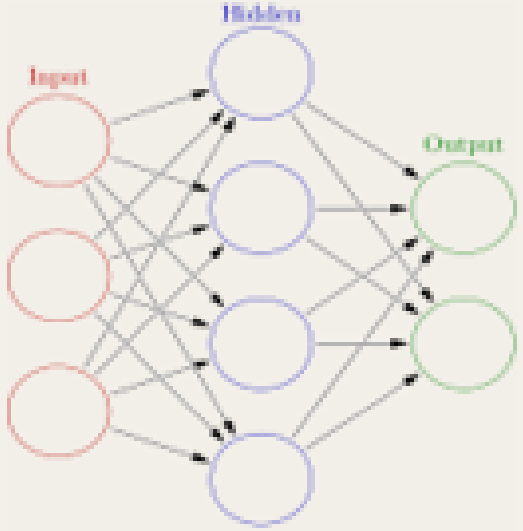
The reduces the overhead on the detection system

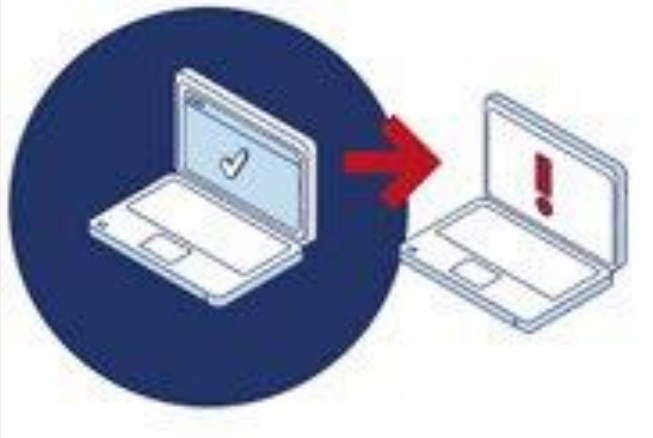
2. Increased accuracy of detection due to two-phase detection

3. Integrable with existing system

4. Active learning model

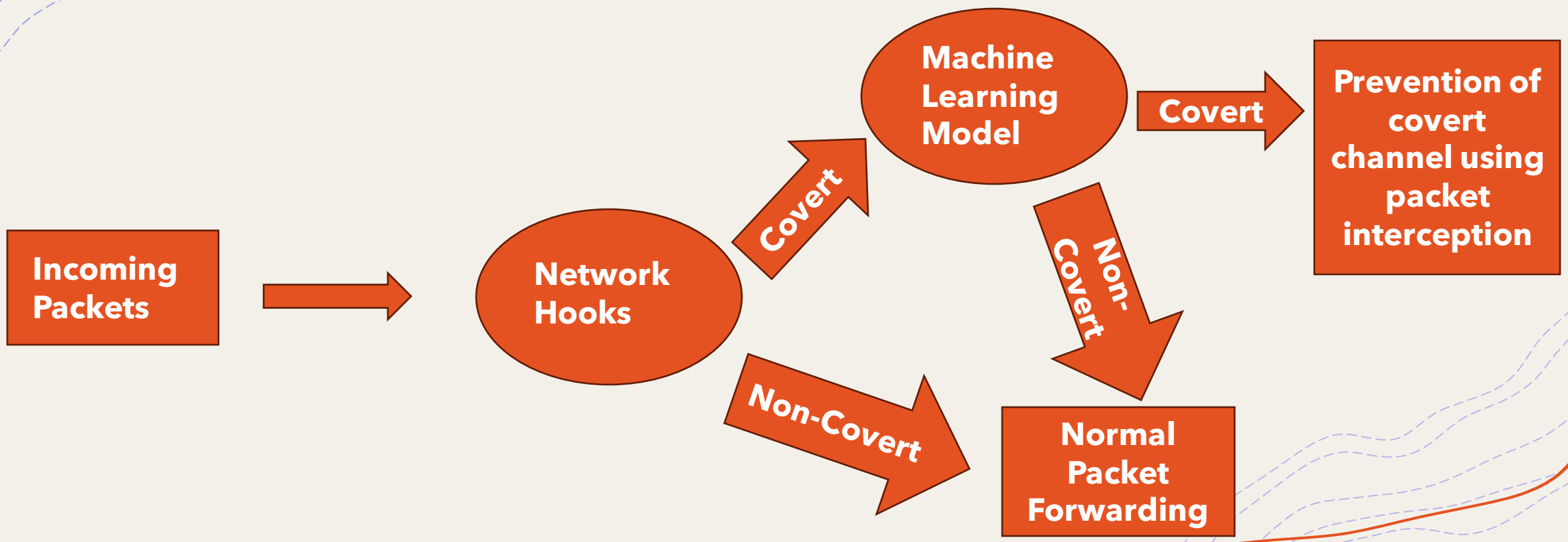
Dependencies and Constraints



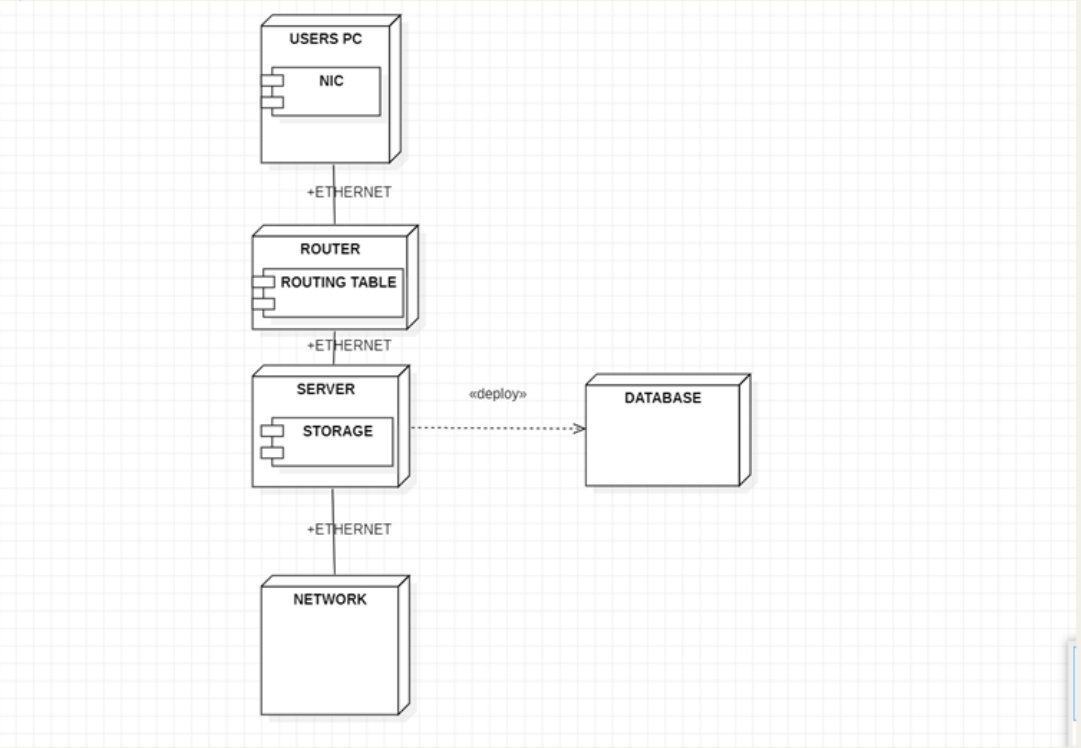


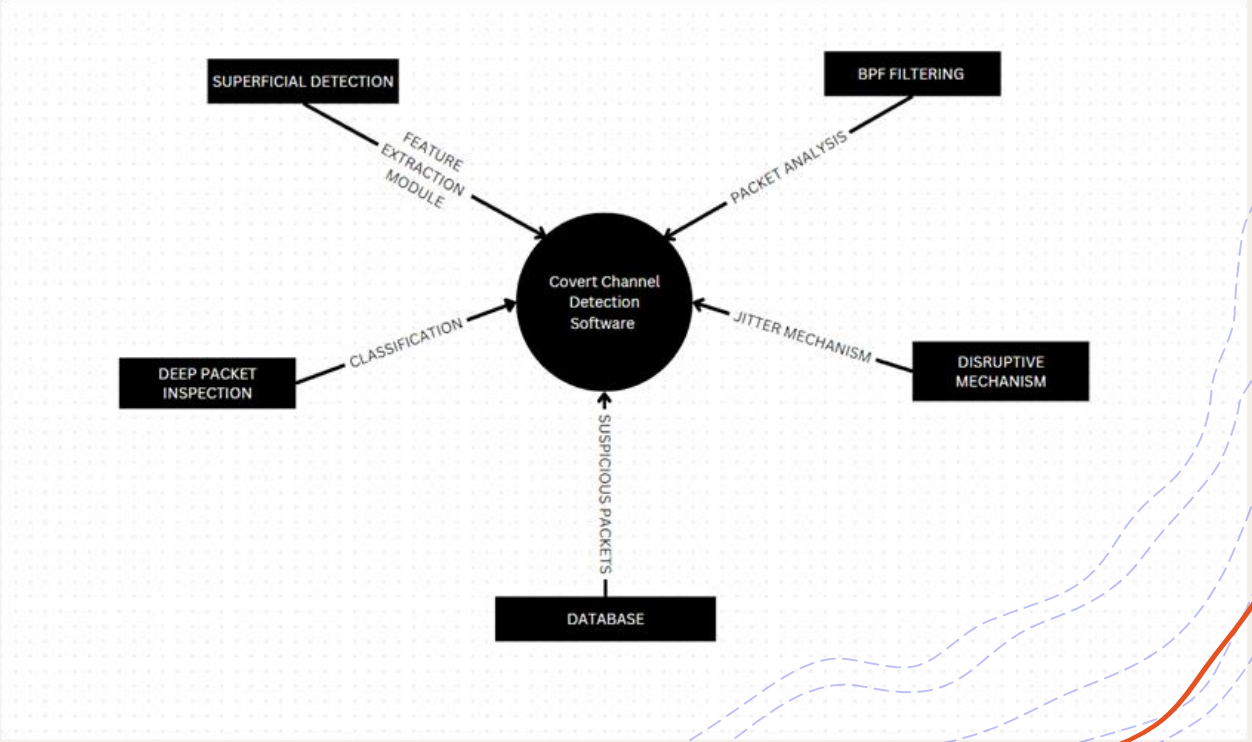
User Groups

Interactions Between Components



Architecture Diagrams





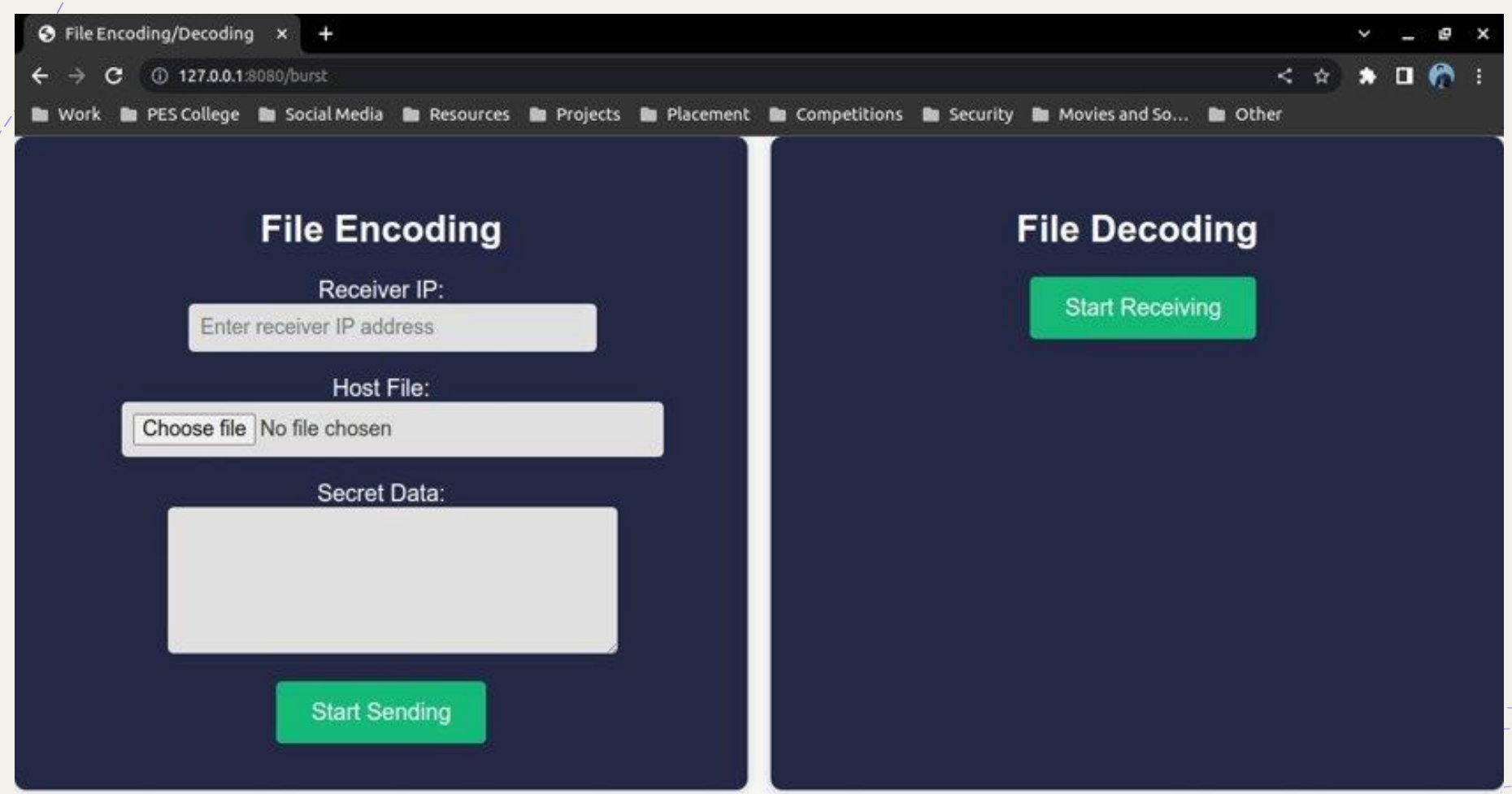
Technologies Used

+ Networking
+ Python
+ Machine Learning
+ Wireshark
+ Virtual machines
+ EBPF
+ Other open-source tools

Project Progress

- Problem statement refining
- Literature Survey
- Writing Survey Paper
- Creation of covert channels
  - Packet burst method
  - TCP Timestamping
- BPF packet filter to capture all packets
- Code for generating dataset for network packets

Project Demo / Walkthrough



Summary of Capstone - I

+ Covert channels can pose a great threat to privacy as they can go undetected. It is very crucial to detect and prevent them.

+ The project mainly focuses on prevention of timing covert channels using 2 level of detection to avoid overhead as well as assure least false positives.

+ With the unavailability of dataset, or the existing open-source technologies in the area, in capstone-I we mainly focused on understanding and creation of covert channel along with automating dataset generation.

Project plans for Capstone Phase - II

+ Dataset generation
+ Analysis of data
+ Data preprocessing
+ Superficial analysis using packet summarizer
+ Training machine learning model
+ Analysis of models
+ Fine tuning of the hyperparameters
+ Writing research paper

Thank You