AI-DRIVEN SUPPLY CHAIN ATTACK DETECTION SYSTEM

AI5063 COURSE PROJECT

GROUP 3

TABLE OF CONTENTS

01

BACKGROUND

SUPPLY CHAINS

- A supply chain encompasses the network of resources, processes, and stakeholders involved in producing and delivering a product or service to end-users.
- A single breach in the supply chain can ripple through multiple products or services, affecting thousands (or millions) of users.

02

DATASET

DATASET

- Few datasets available online (DFRLab)
- Synthetic Dataset Generation Tool
- Features such as Total Lines Changes (Additions and Deletions), Change in avg/max of Directory depth and File Size, Number of Files, Total Repo Size, Presence of Executables, Time since last commit, Upload Time, Dependency Count
- Time-Series Dataset where each package has multiple commits across a period of time

03

AI

AI

- Used CNN Model for Feature Extraction
  - Ideal for pattern recognition in signals.
  - Works well for tasks involving localized patterns.
  - The focus is on detecting local features (e.g., peaks)
  - Patterns are stationary (e.g., they occur at different positions within the signal)
  - Extracts hierarchical features efficiently, capturing local and high-level patterns.

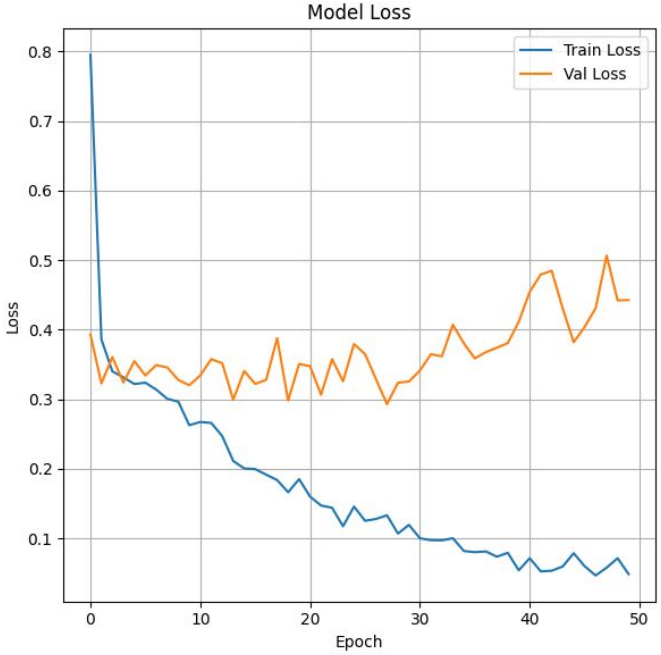
04

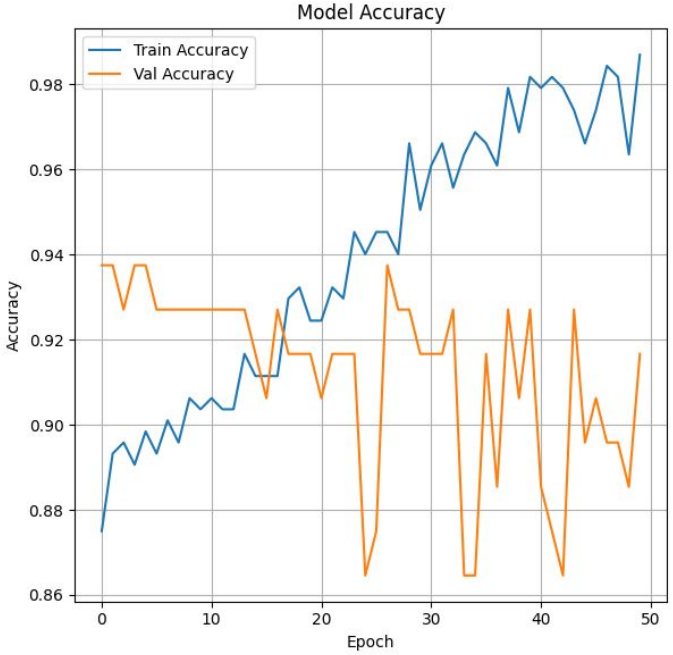
INFERENCE

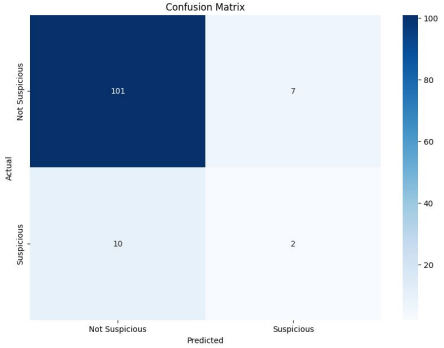
INFERENCE

- Binary Classification
  - Predicting whether package is malicious or not
  - Extracted features, from basic local patterns to higher-level abstractions, are used for robust decision-making between the two classes.

INFERENCE


Model Loss
Train Loss
Val Loss
Loss
Epoch
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
10
20
30
40
50


Model Accuracy
Train Accuracy
Val Accuracy
Accuracy
Epoch
0.98
0.96
0.94
0.92
0.90
0.88
0.86
0
10
20
30
40
50


Confusion Matrix
Not Suspicious
Suspicious
Actual
101
7
10
2
Not Suspicious
Suspicious
Predicted
100
80
60
40
20

05

SERVER + UI

Server + UI

- Static Package Checks like Imports, Hashes
- Repository Checks using our Model
- Submitting Repositories into the Database
- Verification of submitted Repositories by Admin
- List of Packages in the Database
- User Authentication for access to Features

QUESTIONS

GROUP 3

THANK YOU

GROUP 3