Nome dell'applicazione: MalwareDetector AI

Sviluppatori: Matteo Fiacco e Matteo Munetti

Contatti: matteofiacco2@gmail.com e munmatteo@gmail.com

Scopo dell'applicazione:

MalwareDetector AI è un'applicazione basata su intelligenza artificiale progettata per analizzare codice sorgente in forma di stringa al fine di determinare se si tratta di un malware o di un codice sicuro. Utilizza tecniche avanzate di machine learning per identificare pattern comuni di codice dannoso e riconoscere quello sicuro

Tecnologie utilizzate:

- **Linguaggio di programmazione:** Python
- **Framework di intelligenza artificiale:** PyTorch per lo sviluppo e l'addestramento dei modelli di machine learning.
- **Interfaccia grafica:** Opzionale, l'applicazione può essere utilizzata tramite riga di comando o tramite un'interfaccia grafica utente (GUI) per facilitare l'interazione.
- **Modello personalizzato:** Questo è un modello di rete neurale per la classificazione binaria (2 classi di output). È relativamente "piccolo", con un'architettura composta da vari strati lineari (nn.Linear) seguiti da funzioni di attivazione ReLU e dropout per ridurre il rischio di overfitting. Ha una dimensione di input definita dal numero di features dopo la vettorizzazione dei dati di input. È stato addestrato utilizzando l'algoritmo di ottimizzazione Adam e la funzione di loss CrossEntropyLoss. Dopo l'addestramento(avvenuto utilizzando le gpu fornite da seeweb per il contest), è stato valutato su un test set e ha mostrato un'elevata accuratezza(mediamente accuracy a 0.97 e loss a 0.17) che è stata stampata a ogni epoca durante il processo di addestramento.
- **Lista datasets utilizzati:**


XSS_SQL.csv

Funzionalità principali:

1. **Analisi del codice:** MalwareDetector AI accetta una stringa di codice sorgente e la analizza utilizzando un modello di machine learning.
2. **Identificazione dei malware:** Utilizzando l'apprendimento supervisionato, l'applicazione confronta il codice sorgente analizzato con modelli noti di malware per determinare se corrisponde a comportamenti dannosi.
3. **Interfaccia utente:** Fornisce un'interfaccia utente intuitiva, che può essere una GUI, per agevolare l'interazione con l'utente e visualizzare i risultati dell'analisi.

Modalità di utilizzo:

- **Per utlizzare l’applicazione bisogna innanzitutto scaricare le librerie necessarie, che sono:**

  librerie relative all'app python 3.12.0

  - Torch 2.3.0

  - Kivy 2.3.0

  - Kivymd 2.0.1.dev0

  - Scikit-learn 1.4.2

  - Pandas 2.2.2

  Librerie relative al codice del modello python 3.10.12

  - Torch 2.3.0

  - Pandas 2.1.4

  - Scikit-learn 1.3.

- **Da riga di comando o tramite l’interfaccia grafica l'utente può poi utilizzare l’IA passando come argomento la stringa di codice da analizzare.**

Considerazioni sulla sicurezza:

MalwareDetector AI utilizza tecniche avanzate di machine learning per rilevare i malware(ovviamente in minima parte può , ma non garantisce la rilevazione di tutti i tipi di codice dannoso, e’ stata addestrata per riconoscere codesti malware:

-XSS

-SQL injection