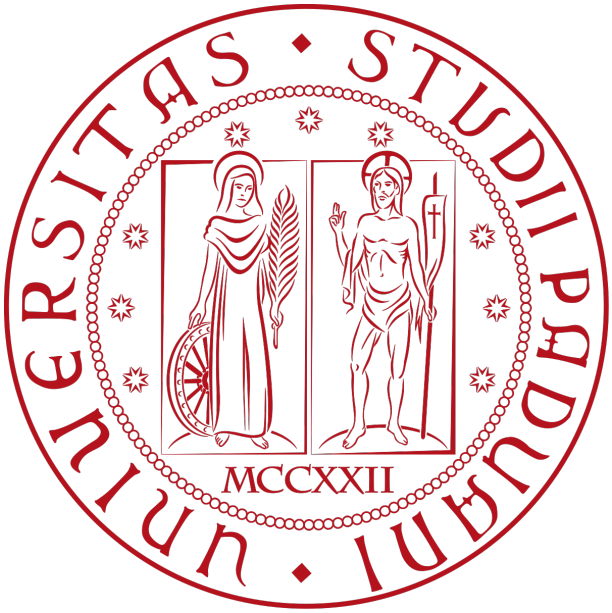
Università degli Studi di Padova



DIPARTIMENTO MATEMATICA

Scuola di Scienze

Corso di Laurea in Informatica

Piano di Lavoro

Contatti
Studente: matteo.tiozzo.1@studenti.unipd.it
Tutor proponente: alessandro.galeazzi@unipd.it
Tutor interno: pvinod21@gmail.com

24/08/2024

Indice

1 Scopo dello stage

Lo scopo di questo progetto di stage è sviluppare un modello avanzato di intelligenza artificiale specializzato nella creazione e nel riconoscimento di malware utilizzando le reti generative avversarie (Generative Adversarial Networks, GAN). Questo progetto mira a sfruttare la potenza delle GAN, che consistono in una rete generativa e una rete discriminante in competizione tra loro, per generare nuovi campioni di malware e, contemporaneamente, migliorare la capacità di rilevamento di tali minacce.

Lo studente contribuirà al miglioramento della sicurezza informatica attraverso l'identificazione precoce e accurata di minacce emergenti che possano compromettere la sicurezza dei dispositivi e delle reti. Il progetto non solo intende affinare le tecniche di rilevamento dei malware esistenti, ma anche esplorare nuovi approcci innovativi per anticipare possibili varianti di malware ancora sconosciute. In ultima analisi, il progetto aspira a rafforzare le difese informatiche mediante lo sviluppo di strumenti intelligenti in grado di adattarsi rapidamente all'evoluzione delle minacce digitali, rendendo l'ambiente informatico più sicuro e resiliente.

2 Periodo

- Data prevista di inizio: 08/09/2024
- Data prevista di fine: 08/11/2024

3 Interazione tra tirocinante e tutor aziendale

Sono pianificati incontri periodici con il tutor aziendale per discutere lo stato di avanzamento del progetto, aggiornare gli obiettivi, se necessario, e risolvere eventuali dubbi. Il tutor sarà inoltre disponibile su richiesta per rispondere a domande, fornire supporto operativo durante l'intero svolgimento del progetto e garantire che il piano di lavoro rimanga aggiornato. Le comunicazioni avverranno tramite i canali principali concordati, con la possibilità di colloqui in presenza qualora si rendesse necessario un confronto diretto.

4 Prodotti attesi

Lo studente sarà responsabile di documentare quotidianamente il lavoro svolto e di confrontare i progressi ottenuti con quelli previsti. Al termine del periodo di stage, dovrà redigere una relazione scritta dettagliata che illustri il percorso seguito e i risultati conseguiti. In particolare, la relazione dovrà includere:

- Le conclusioni emerse dallo studio del problema e dalla ricerca bibliografica
- L'analisi del corpus utilizzato durante tutto lo stage
- La documentazione completa dei modelli sviluppati, in modo da garantire la replicabilità dei risultati ottenuti

5 Obiettivi

Notazione

Si farà riferimento ai requisiti secondo le seguenti notazioni:

1. ***O***: obbligatorio, vincolo irrinunciabile
2. ***D***: desiderabile, vincolo non strettaente necessario, ma che da valore aggiunto al prodotto

Le sigle precendentemente descritte saranno seguite da un numero progressivo per identificare univocamente il requisito.

Obiettivi fissati

Si prevede lo svolgimento degli obiettivi riportati sotto.

- Obbligatori:
  - ***O1***: studio del problema e ricerca in letteratura
  - ***O2***: implementazione e sperimentazione di modelli di GAN
  - ***O3***: documentazione dei modelli sviluppati, con relativo repository git
- Desiderabili:
  - ***D1***:

6 Pianificazione del lavoro

Pianificazione settimanale

- **Settimana 1 (40 ore)**
  - Preparazione dell'ambiente di sviluppo
  - Studio teorico sul problema e sull'utilizzo delle Generative Adversarial Network (GAN) in merito
- **Settimana 2 (40 ore)**
  - Studio teorico sul problema e sull'utilizzo delle Generative Adversarial Network (GAN) in merito
  - Ricerca teorica delle ultime vulnerabilità riscontrate su sistema operativo iOS
- **Settimana 3 (40 ore)**
  - Ricerca di dataset per l'addestramento dei modelli
  - Ricerca di modelli GAN
- **Settimana 4 (40 ore)**
  - Implementazione di modelli di GAN
- **Settimana 5 (40 ore)**
  - Sperimentazione e verifica dei modelli implementati
- **Settimana 6 (40 ore)**
  - Soluzione degli errori e delle problematiche riscontrate
- **Settimana 7 (40 ore)**
  - Documentazione dei modelli sviluppati
- **Settimana 8 (20 ore)**
  - Scrittura della tesi

7 Ripartizione delle ore

Durata in ore	Descrizione attività
75	Formazione sul problema e sugli algoritmi di machine learning
150	Implementazione degli algoritmi, ottimizzazione degli stessi e correzione di possibili errori
75	Stesura documentazione e scrittura tesi
Totale ore	**300**

Approvazione

Il presente piano di lavoro è stato approvato dai seguenti soggetti:

Galeazzi Alessandro Tutor proponente

Tiozzo Matteo Stagista

Possibile tutor interno (Vinod)