UNIVERSITÀ DI PISA

ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY

FRANCESCO MARCELLONI

Anno accademico	2021/22
CdS	CYBERSECURITY
Codice	931II
CFU	6

Moduli	Settore/i	Tipo	Ore	Docente/i
ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY	ING-INF/05	LEZIONI	48	GIANLUCA DINI FRANCESCO MARCELLONI

Obiettivi di apprendimento

Conoscenze
Gli studenti che completeranno con successo l'insegnamento avranno una conoscenza di base delle principali tecniche di pre-processazione dei dati, classificazione, predizione, clustering, outlier detection e estrazione dei pattern frequenti. Questa conoscenza permetterà loro di affrontare problemi di cybersecurity (Spam Detection, Fraudulent Transaction Detection, Anomaly Detection, Malware Analysis, Network Traffic Analysis) con tecniche di artificial intelligence e di identificare la tecnica più adatta per risolverli.

Modalità di verifica delle conoscenze
Durante la verifica delle conoscenze, gli studenti devono dimostrare di aver appreso le diverse tecniche insegnate durante lo svolgimento del corso e devono essere capaci di identificare la soluzione più adatta per problemi specifici di cybersecurity.
I metodi sono:

- esame orale
- report e presentazione di un progetto

Ulteriori informazioni: allo studente è richiesto di sviluppare un progetto in cui vengono utilizzate tecniche di artificial inteligence per risolvere problemi di cybersecurity. I risultati del progetto vengono discussi durante una presentazione.

Capacità
Al termine del corso,

- lo studente saprà affrontare i più comuni problemi di cybersecurity, trovando le soluzioni basate sull'intelligenza artificiale più idonee per risolverli
- lo studente saprà valutare e confrontare più soluzioni e scegliere la più adatta

Modalità di verifica delle capacità
Lo studente dovrà preparare e presentare una relazione scritta che riporti i risultati dell'attività di progetto

Comportamenti
Lo studente potrà acquisire un metodo per affrontare problemi di cybersecurity con tecniche di intelligenza artificiale e per selezionare le migliori soluzioni da adottare

Modalità di verifica dei comportamenti
Durante le sessioni di laboratorio saranno valutati il grado di accuratezza e precisione delle attività svolte dallo studente
Durante lo sviluppo del progetto saranno verificate le modalità di gestione e organizzazione delle fasi progettuali

Prerequisiti (conoscenze iniziali)
Conoscenze di base di matematica
Conoscenze di linguaggi di programmazione

Indicazioni metodologiche

Le lezioni verranno svolte frontalmente con l'ausilio di lucidi
Le esercitazioni verranno svolte in laboratorio con l'ausilio di lucidi
Durante il corso, verrà sviluppato dallo studente un progetto che costituirà parte della valutazione finale

L'intero corso è tenuto in Inglese

Programma (contenuti dell'insegnamento)

Data Preprocessing: data cleaning, integration, reduction, transformation and discretization.
Classification: basic concepts, decision tree induction, Bayes classification methods, lazy learners, techniques for improving accuracy, model evaluation and selection.
Clustering: basic concepts, partitioning methods, hierarchical methods, density-based methods, model evaluation and selection.
Outlier detection: statistical, proximity-based, clustering-based and classification-based approaches.
Frequent pattern mining: basic concepts, A-priori algorithm, pattern evaluation methods.
Examples of application of the artificial intelligence techniques described during the lectures to typical cybersecurity problems such as spam detection, fraudulent transaction detection, anomaly detection, malware analysis, network traffic analysis will be also discussed.

Bibliografia e materiale didattico

J Han and M Kamber Data Mining Concepts and Techniques Morgan Kaufmann, 3 rd ed 2011

C Chio and D Freeman, Machine Learning and Security Protecting Systems with Data and Algorithms, O'Really Media, Inc 2018

A Parisi Hands on Artificial Intelligence for Cybersecurity, Packt Publishing, 2019

Papers on the different algorithms described during the course

Slides

Modalità d'esame

L'esame è composto dalla discussione del progetto e una prova orale.
La discussione del progetto viene tipicamente tenuta qualche giorno prima dell'esame orale. Il candidato deve presentare come il progetto è stato sviluppato, motivare le sue scelte progettuali e discutere i risultati ottenuti. Il progetto viene valutato positivamente se il candidato mostra di aver seguito un approccio corretto e di aver valutato in modo critico le possibili soluzioni, scegliendo la più appropriata
La prova orale consiste in un colloquio tra il candidato e il docente sugli argomenti trattati a lezione.
La prova orale è superata se il candidato mostra padronanza degli argomenti trattati, si esprime in modo chiaro e con terminologia corretta, mostra capacità di analisi e sintesi.

Stage e tirocini

Ultimo aggiornamento 21/11/2021 18:12