

Un sistema di recommendation per la cybersecurity basato su Collaborative Filter

Andrea Michele Albonico

24 Febbraio 2020

Il mondo del Cloud ha portato molti benefici, tuttavia solleva diverse problematiche legate alla **mancaanza di fiducia**

- Non vengono fornite agli utenti le specifiche riguardanti le misure di sicurezza messe in atto
- Sono sistemi specifici e **difficili da utilizzare** se non si ha esperienza in materia

Scenario e Motivazioni (2)

Moon Cloud è una piattaforma erogata come servizio, la quale supporta:

- un sistema di *Security Governance*
- un framework di *Security Assurance*



Garantisce il controllo della sicurezza informatica in modo rapido ed efficiente, attraverso attività di test e monitoraggio periodiche e programmate

Introdurre un **sistema di raccomandazione** che possa consigliare all'utente delle possibili *Evaluation* rispetto all'*asset* indicato da proteggere e monitorare

- L'utente meno esperto può usufruire dei servizi offerti da Moon Cloud in modo **semplice** e **intuitivo**
- Si è cercato di colmare il problema della mancata fiducia in questi sistemi

Un *recommendation system* può filtrare i dati usando differenti algoritmi e raccomandare gli item più rilevanti agli utenti attraverso un procedimento a 3 fasi

- 1 **Raccolta di dati:** ottenere dati rilevanti e consistenti su cui applicare algoritmi di raccomandazione
- 2 **Memorizzazione di dati:** la quantità di dati definisce quanto efficace un modello di raccomandazione può diventare
- 3 **Filtraggio dei dati:** estrarre le informazioni più rilevanti

Questo sistema tenta di predire la preferenza che un utente darebbe a un item basandosi sulle preferenze date da altri utenti

- Memory-based: metodi che mirano a determinare il grado di relazione tra utenti e item identificando utenti con uno storico di item usati simile
 - ▶ **UB-CF**: algoritmo che fornisce dei suggerimenti sulla base di uno o più vicini (*neighbours*)
 - ▶ **IB-CF**: algoritmo che confronta gli item dell'utente a cui si vuole raccomandare e i possibili item simili
- Hybrid filter: combinare più tecniche di raccomandazione, raggruppando i pregi di ciascun approccio

Collaborative filtering (2)

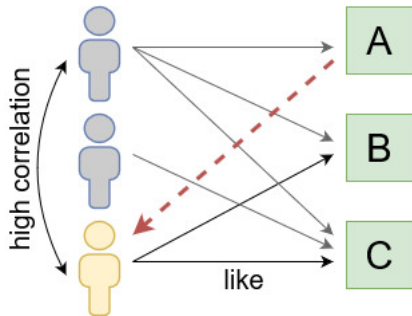


Figura: User based Collaborative Filter

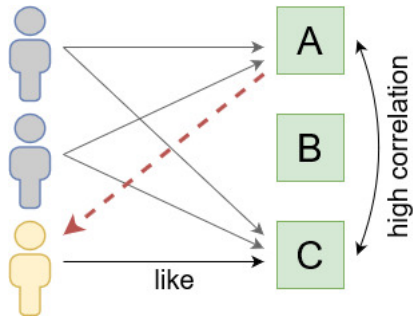
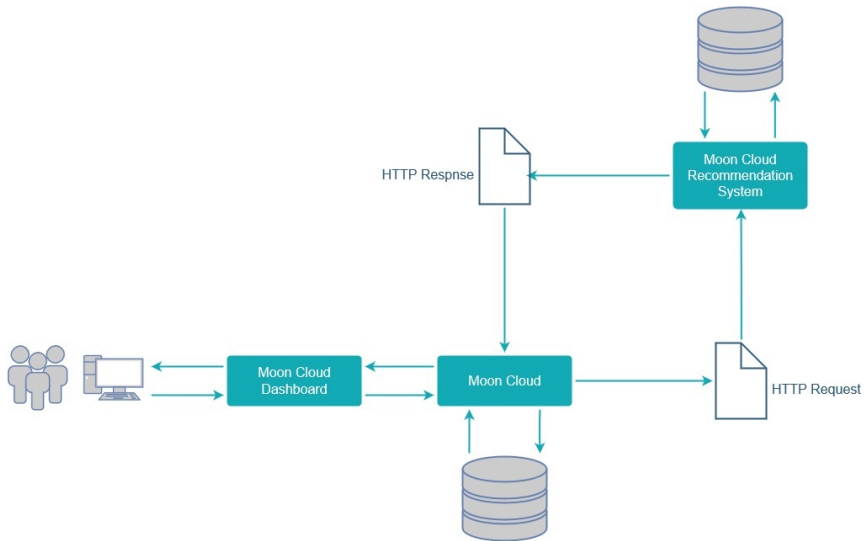


Figura: Item based Collaborative Filter

Servizio di **API REST**, che si appoggia a un database Postgres, accessibile attraverso apposite URL; questo servizio permette di effettuare richieste al sistema di raccomandazione e di aggiornare la base di dati

- 1 Preparazione della base di dati
- 2 Realizzazione delle View
- 3 Consistenza tra i database
- 4 Deployment in Docker

Soluzione (2)



La soluzione proposta introduce un sistema di raccomandazione in un mondo in cui spesso non è presente perché popolato da utenti esperti

- viene data una possibilità a un **maggior numero di utenti** di accedere a servizi su un sistema Cloud di Security Assurance in totale sicurezza e affidabilità