

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

- poca fiducia da parte degli utenti in questi sistemi
- col tempo sono diventati molto complessi e impegnativi da gestire, soprattutto dal punto di vista della sicurezza
- sono sistemi specifici e difficili da utilizzare se non si ha esperienza in materia

Introduzione di un **sistema di raccomandazione** che possa consigliare all'utente delle possibili *Evaluation* rispetto all'*asset* che vuole 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

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

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 informazioni 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

Collaborative filtering

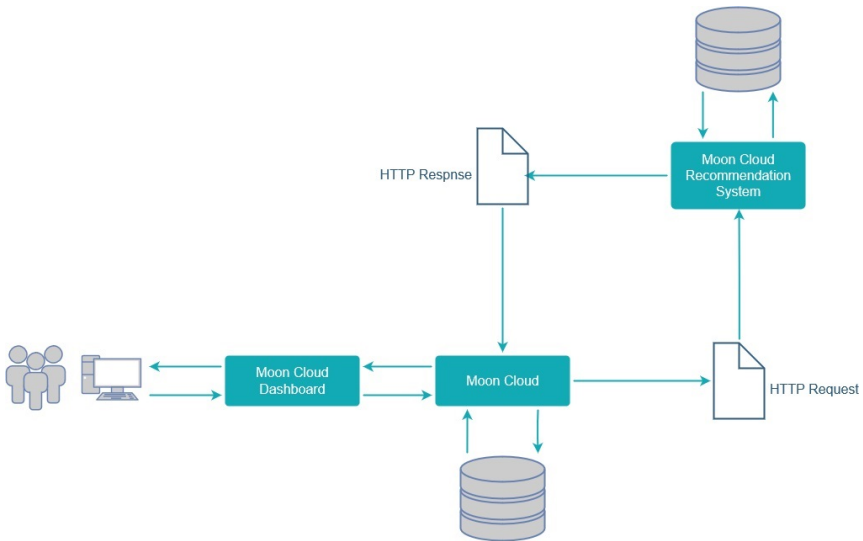
Questo sistema predice la preferenza che un utente accorderebbe a un item basandosi sulle preferenze date da altri utenti

- **semplici da implementare, intuitivi** e non necessitano di operazioni di training sui dati e regolazione di molti parametri
- permettono all'utente di comprendere le ragioni che si celano dietro ad ogni raccomandazione

Servizio di **API REST** accessibile attraverso apposite URL che 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 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 di test e monitoraggio in totale sicurezza e affidabilità