Un sistema di recommendation per la cybersecurity basato su Collaborative Filter

Andrea Michele Albonico

24 Febbraio 2020

Scenario e Motivazioni

Il mondo del Cloud ha portato molti benefici, tuttavia solleva diverse problematiche legate alla mancanza 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

Obiettivo della tesi

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

Sistema di raccomandazione

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

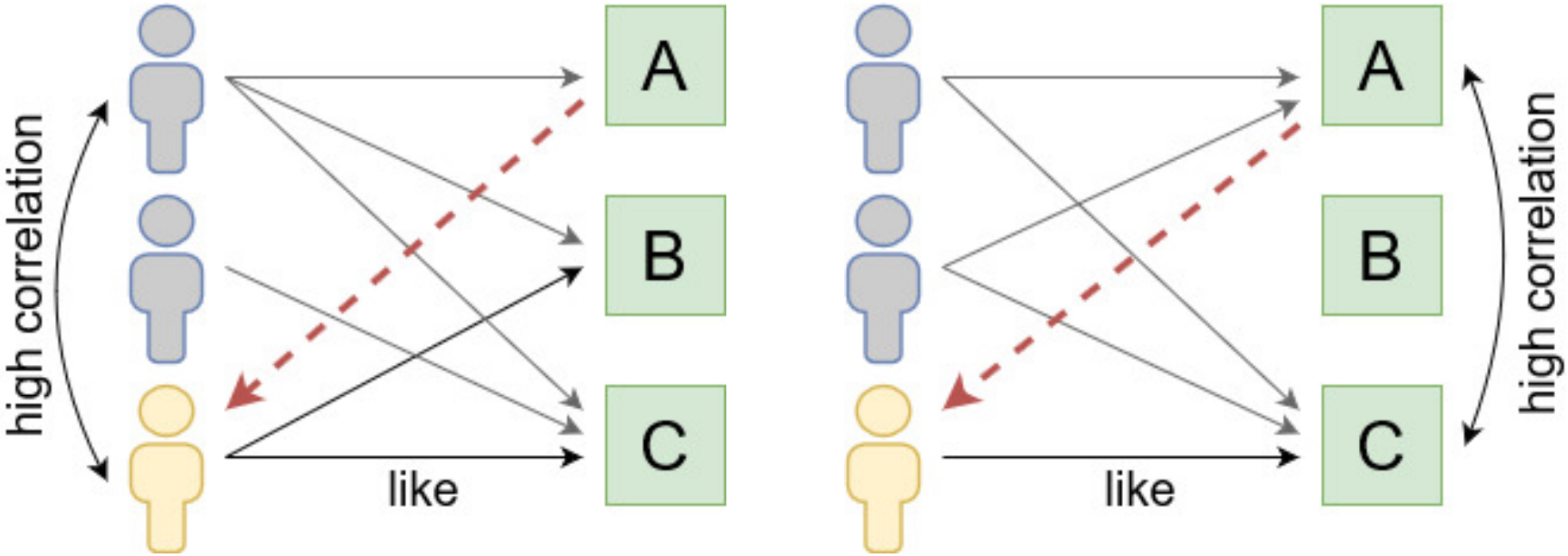
1. Raccolta di dati: ottenere dati rilevanti e consistenti su cui applicare algoritmi di raccomandazione
2. Memorizzazione di dati: la quantità di dati definisce quanto efficace un modello di raccomandazione può di diventare
3. Filtraggio dei dati: estrarre le informazioni più rilevanti

Collaborative filtering

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

- 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: combinazione di più tecniche di raccomandazione per raggruppare i pregi di ciascun approccio

Collaborative filtering (2)

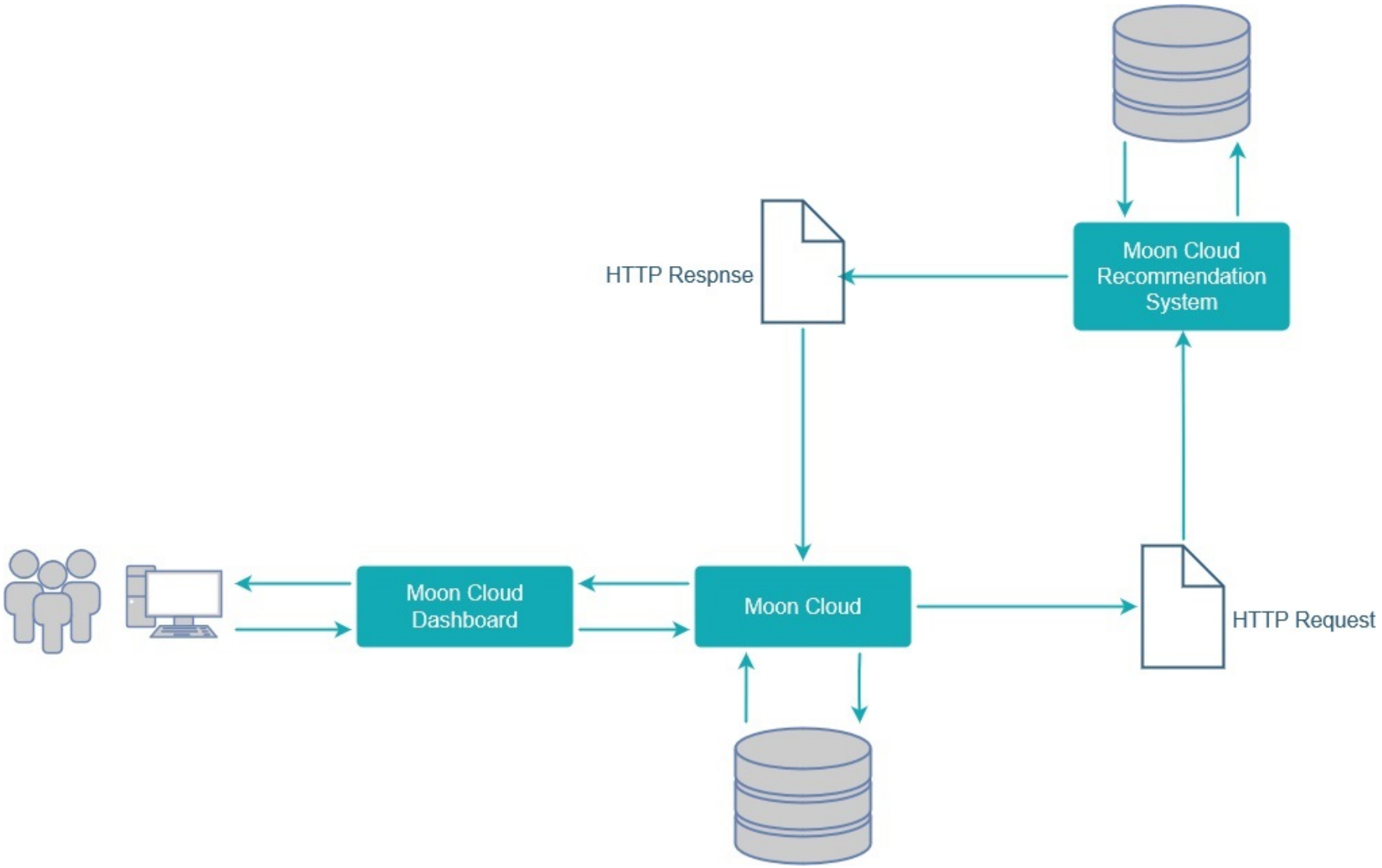


Soluzione

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)


HTTP Respnse
Moon Cloud Recommendation System
Moon Cloud Dashboard
Moon Cloud
HTTP Request

Conclusioni

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