Verbale Interno del meeting in data

A.A 2024/2025

sevenbits.swe.unipd@gmail.com

Registro modifiche

Versione	Data	Autore	Verificatore	Descrizione
0.1.0	2025-01-08	Leonardo Trolese	Alfredo Rubino	Redazione del verbale

Indice

1 Data

1.1 Durata e partecipanti

- Ora: 17:00 - 17.:25;
- Partecipanti:
  - SevenBits:
    - Gusella Manuel
    - Peruzzi Uncas
    - Piva Riccardo
    - Pivetta Federico
    - Rubino Alfredo
    - Cristellon Giovanni
    - Trolese Leonardo
  - SyncLab:
    - Dorigo Andrea
    - Pallaro Fabio
    - Zorzi Daniele
- Piattaforma: Google meet (online)

1.2 Oggetto

Quarto SAL con Dorigo Andrea, Pallaro Fabio e Zorzi Daniele di SyncLab.

1.3 Sintesi

Durante il quarto SAL il proponente è stato messo al corrente dello stato del progetto: sono state esposte le novità implementate nel PoC ed è stato esposto quanto prodotto dal punto di vista della documentazione fino ad ora. Relativamente al Proof of Concept il gruppo ha esposto un problema rilevato alla creazione dei topic Kafka e la relativa soluzione adottata; il team ha infine confermato di avere completato l'implementazione del PoC in vista della RTB. Nella fase finale della riunione è stato discusso un dubbio emerso durante il colloquio del gruppo con il professor Cardin relativo alla sicurezza del software in produzione.

1.4 Domande

E' stato posto un unico dubbio:

1. E' necessario adottare una soluzione che mitighi o risolva il problema di sicurezza del potenziale Kafka Poisoning, ovvero del possibile invio di dati nocivi per il sistema attraverso Kafka?

1.5 Risposte

1. Il focus del progetto è la generazione di messaggi pubblicitari personalizzati mediante IA, pertanto, sebbene il problema esposto andrebbe sicuramente affrontato e risolto in un contesto reale, non è necessario che ciò venga fatto nel contesto del progetto in questione. Si suggerisce comunque al gruppo di studiare autonomamente il problema e le possibili soluzioni ad esso, valutando la fattibilità dell'adozione di ognuna di esse rispetto al tempo a disposizione per il completamento del progetto. Se il gruppo valutasse accettabile l'impegno orario dato dall'adozione di una di queste soluzioni allora il proponente acconsentirebbe alla sua implementazione.

1.6 Considerazioni sulla sicurezza

A seguito della domanda sul potenziale Kafka Poisoning il proponente ha esposto tre possibili soluzioni al problema da approfondire per il gruppo:

- Encryption: crittografia dei dati in transito per proteggere il sistema da attacchi del tipo man-in-the-middle, oppure a risposo per proteggere i dati anche da attaccanti che hanno accesso ai dati salvati. Si possono configurare i broker Kafka per richiedere connessioni sicure tramite SSL/TLS.
- Authentication: limitare l'accesso al servizio ai soli client autorizzati. Si può realizzare attraverso SASL o MSA.
- Access Control: definire dei permessi specifici garantendo che anche un client compromesso non possa causare danni al sistema.

Il proponente ha quindi suggerito la possibilità di introdurre uno strato di controllo che si limiti a verificare la validità dai dat ricevuti dai sensori, garantendo la loro coerenza. Questa funzionalità non è da considerasi però una soluzione per il Kafka Poisoning, che non può essere prevenuto così facilmente.

1.7 Decisioni prese

E' stato deciso di terminare la redazione degli ultimi dettagli dei documenti, e di fissare quanto prima la revisione RTB con il committente, è stato dato il compito al gruppo di studiare le possibili soluzioni per i problemi di sicurezza in preparazione a una discussione su di esse che avverrà nel successivo SAL, e infine è si è scelto di non fissare una data precisa per il prossimo incontro per via delle incertezze relative a quando si svolgerà la consegna RTB.

2 Obiettivi prossimo SAL

Gli obiettivi stabiliti per il prossimo SAL sono:

- Studio soluzioni per il Kafka Poisoning
- Conclusione documentazione per RTB

Rif.Issue	**Dettaglio Decisione**
Issue #18	Studio delle possibili soluzioni del Kafka Poisining
Issue #19	Studio encryption dei dati in transito
Issue #20	Studio access control dei client
Issue #21	Studio authentication dei client
Issue #111	Redazione verbale esterno 2025-01-08

Firma: _____

Data: .....