## Descrizione della problematica o del bisogno nell'azienda o pubblica amministrazione utente.

La **diffusione dei servizi di Internet banking** e nuovi sistemi di pagamento ha portato a un aumento di **quantità e sofisticazione delle frodi dispositive**—per una perdita di milioni di euro ogni anno—da cui emerge la necessità di **infrastrutture di difesa robuste**. BankSealer soddisfa tale **bisogno** velocizzando l'individuazione di frodi offrendo informazioni contestuali per comprenderne le cause.

## Descrizione della soluzione tecnologica (tecnologie usate, architettura, ecc.).

BankSealer è un **sistema di supporto alle decisioni** per analisi e **rilevazione automatica di frodi** che sintetizza l'interazione di ciascun cliente con il sistema di e-banking, sfruttando avanzate **tecniche statistiche e di machine learning** per rilevare se (e in che modo) una transazione è atipica. In dettaglio, BankSealer "apprende" un modello locale (cliente), globale (filiale) e temporale aggregando i **dati storici delle transazioni**, e ordina le nuove transazioni per "grado di **anomalia**" rispetto ai suddetti modelli.
Il prototipo, già **operativo presso uno dei maggiori gruppi bancari italiani**, ha una struttura modulare e si configura sia "stand alone", sia come "plugin" facilmente integrabile e affiancabile ai sistemi antifrode già in essere.
I componenti principali di BankSealer sono:

1. **Interfaccia Utente**, lo strato di visualizzazione che permette di mostrare all'analista bancario i risultati dell'elaborazione. Tale componente è stata realizzata con React, un framework web ad **alte prestazioni** sviluppato e promosso da Facebook, per minimizzare i costi di rilascio e manutenzione, pur mantenendo un **alto grado di sicurezza** grazie alla connessione HTTPS.
2. **Driver**, realizzato ad-hoc per ogni cliente per integrarsi con l'infrastruttura IT già in essere al fine di **raccogliere efficientemente i dati** da analizzare, e inviare i risultati dell'analisi ad altri eventuali sistemi di raccolta dati a valle. È un componente leggero e flessibile, **grande punto di forza di BankSealer**.
3. **Core Engine**, o livello applicativo vero e proprio, che implementa l'elaborazione delle transazioni. È realizzato in **Scala**, un linguaggio moderno **ampiamente usato** per la sua affidabilità, facilità di rilascio e altissime prestazioni per l'analisi di grandi quantità di dati, grazie a numerose librerie disponibili, e al paradigma di computazione funzionale.
4. **Database**, per lo storage dei dati relativi alle transazioni e dei risultati. Per tale componente è stato selezionato MySQL sia per facilità di integrazione che per semplicità di rilascio e manutenzione.

## Descrizione del progetto di implementazione - complessità, tempi, aspetti organizzativi, costi, ecc.

**Modalità di rilascio**:

- **Stand alone:** ha una sua interfaccia grafica e va "collegato" ai database della banca installando in loco engine e driver. Può essere configurato su una macchina "server grade". I tempi di implementazione stimati in base all'esperienza pregressa sono di 15-20gg. Grazie all'interfaccia web intuitiva, 1–2g di training sono sufficienti per un'operatività iniziale dell'analista.
- **Plug-in:** viene installato l'engine collegato ai database tramite driver custom. Attraverso le API REST (over HTTPS) BankSealer si collega alla dashboard antifrode in essere presso il cliente, per permettere l'inserimento dei nostri risultati direttamente nel cruscotto centralizzato. I tempi di rilascio dipendono dal grado di accoppiamento dell'infrastruttura esistente.

**Costi:**

- costo di licenza annuale della soluzione: 250.000 € (ancora da definire, i competitor partono da costi di listino di 400.000 €/anno a salire)
- costo di integrazione per la versione plug-in: da valutare secondo i tempi su indicati
- eventuali costi di personalizzazione successivi.

## Descrizione dei principali benefici raggiunti dall'azienda o pubblica amministrazione utente.

I principali **benefici** sono:

- **Economici**
  - aumento numero di frodi rilevate (+30%)
  - riduzione perdite derivanti da frodi
  - riduzione tempo necessario per investigare ciascuna segnalazione
  - riduzione contenziosi con i Clienti
- **Threat intelligence**
  - Indagine di ogni segnalazione
    - risultati facilmente interpretabili
  - Fornisce informazioni di "intelligence" riguardo potenziali sorgenti di attacchi informatici
- **Sistema adattabile,** che **evolve**
  - impara dalle scelte degli analisti migliorando le proprie performance nell'individuazione delle frodi
- **Facilità di integrazione**
  - design fortemente disaccoppiato
  - indipendenza dalla sorgente di dati.

## Descrizione degli elementi distintivi e di reale innovatività/originalità della soluzione, anche con riferimento a soluzioni «concorrenti».

1) Prototipo nato nell'ambito della ricerca con base scientifica e focalizzato sulla qualità dei risultati (detection rate ~95%)
2) Sviluppato in collaborazione con un gruppo bancario italiano, provato sul campo integrando i feedback ricevuti dagli analisti.
3) Soluzione basata su un approccio white-box, con risultati facilmente interpretabili. I concorrenti segnalano la sospetta frode senza fornire dettagliate informazioni contestuali. BankSealer non solo fornisce dettagli sull'origine di ogni frode, ma consente anche all'analista di approfondire l'indagine direttamente dall'interfaccia.
4) Sistema leggero, scalabile e centralizzabile che si configura sia stand alone che come un plug-in multi-piattaforma, basato su API facilmente integrabili nei sistemi esistenti.
5) Meno costoso dei prodotti concorrenti: minori costi di licenza, organizzativi e di integrazione.