AuthMe:

Autenticazione continua su smartphone tramite accelerometro e giroscopio

Prof. Donato Impedovo
Dott. Vincenzo Gattulli

Gabriele Grieco

Indice

Introduzione

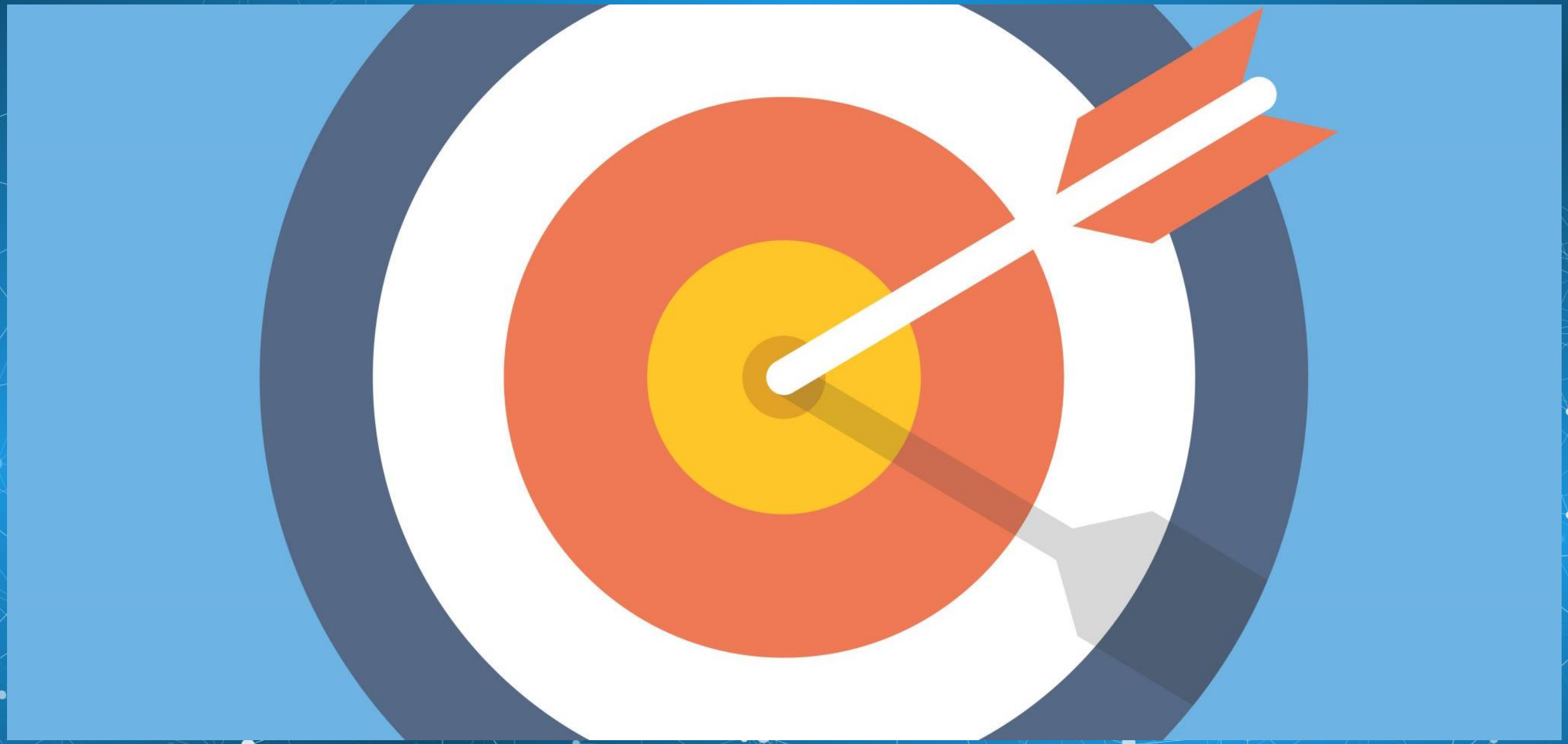
ISLab Intelligent Systems Laboratory

Introduzione

Ogni individuo è unico ed ha un suo modo di interagire con il dispositivo.

Diverse tecniche di biometria comportamentale sono:

- Signature analysis
- Gait Recognition;
- Keystroke Dynamics (KD);
- Mobile Biometrics;
- etc.



Obiettivo

ISLab Intelligent Systems Laboratory

Obiettivo

AuthMe si basa sul Motion Dynamics,

- autenticazione/identificazione continua su smartphone sfruttando i dati provenienti da **Accelerometro** e **Giroscopio;**
- calcolando:
  - features temporali;
  - features di frequenza;
- riducendo, per quanto possibile, il costo computazionale;
- utilizzo di algoritmi di machine learning, one-class e multi-class;
- autenticazione continua ogni t secondi $t \in [0.2s, 5s]$

Stato dell’Arte

ISLab Intelligent Systems Laboratory

Stato dell’Arte

Il paper dal quale si è preso spunto è «Multisensor-Based Continuous Authentication of Smartphone Users With Two-Stage Feature Extraction»

In questo esperimento hanno raggiunto ottimi risultati servendosi di una **doppia features extraction** dai dati dei sensori inerziali:

1. estrazione manuale;
2. Deep Metric Learning.

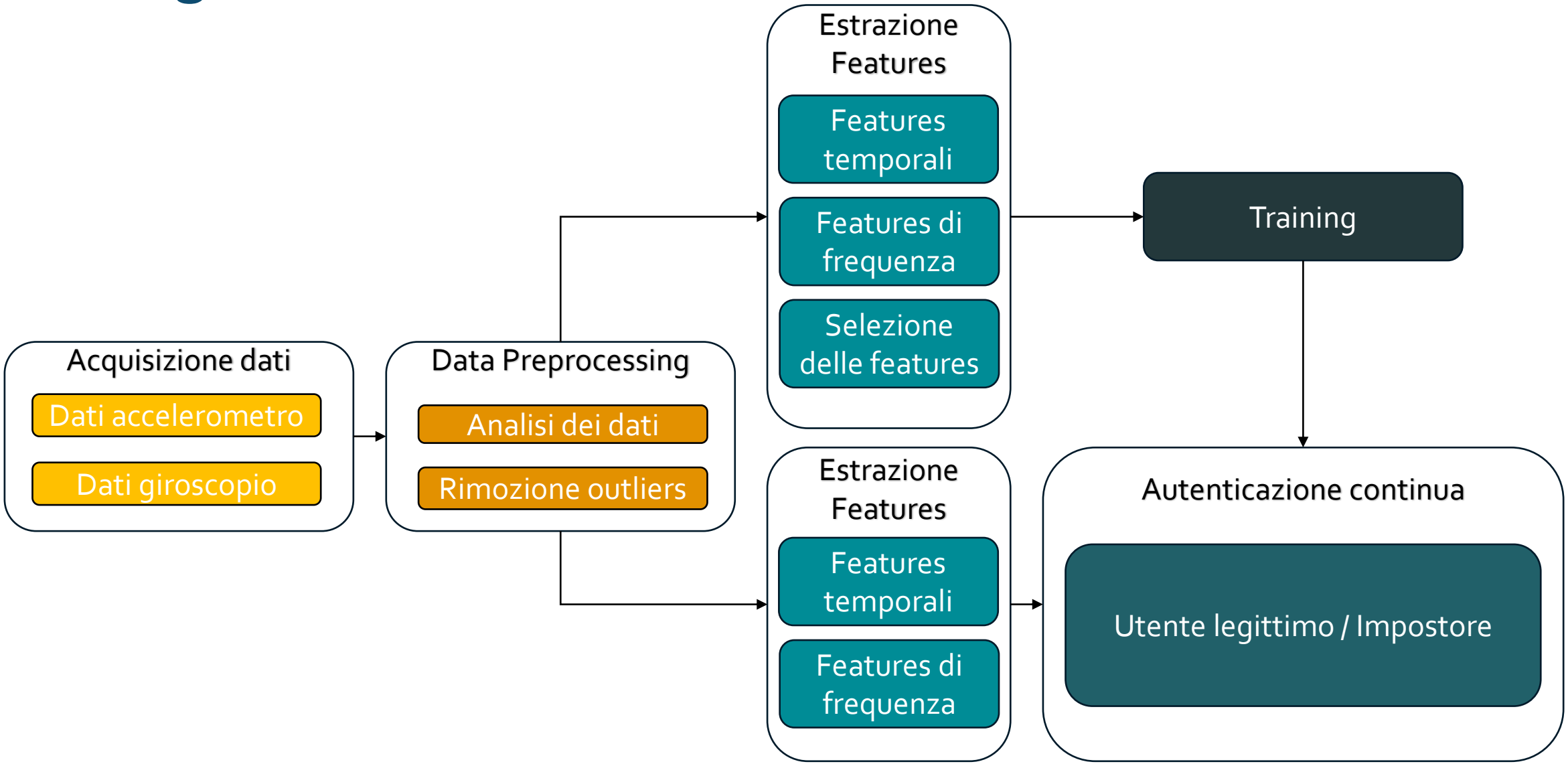
Questi hanno identificato le features più rilevanti per poi utilizzarle in vari modelli di machine learning one class.

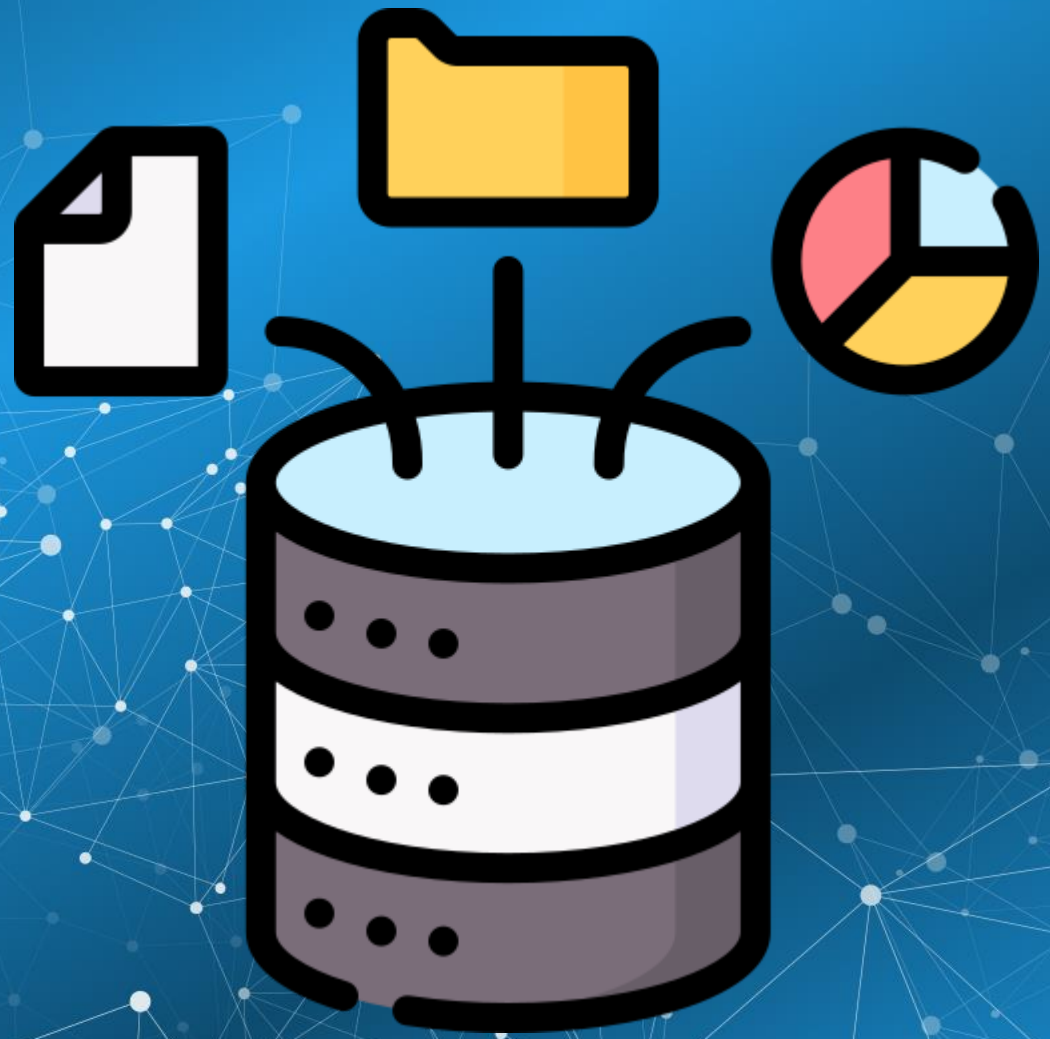
[Multisensor-Based Continuous Authentication of Smartphone Users With Two-Stage Feature Extraction», *IEEE Internet Things J*, vol. 10, n. 6, pagg. 4708–4724, mar. 2023, doi: 10.1109/JIOT.2022.3219135.]

Design

ISLab Intelligent Systems Laboratory

Design


Acquisizione dati
Dati accelerometro
Dati giroscopio
Data Preprocessing
Analisi dei dati
Rimozione outliers
Estrazione Features
Features temporali
Features di frequenza
Selezione delle features
Estrazione Features
Features temporali
Features di frequenza
Training
Autenticazione continua
Utente legittimo / Impostore



Datasets

ISLab Intelligent Systems Laboratory

Dataset: BrainRun

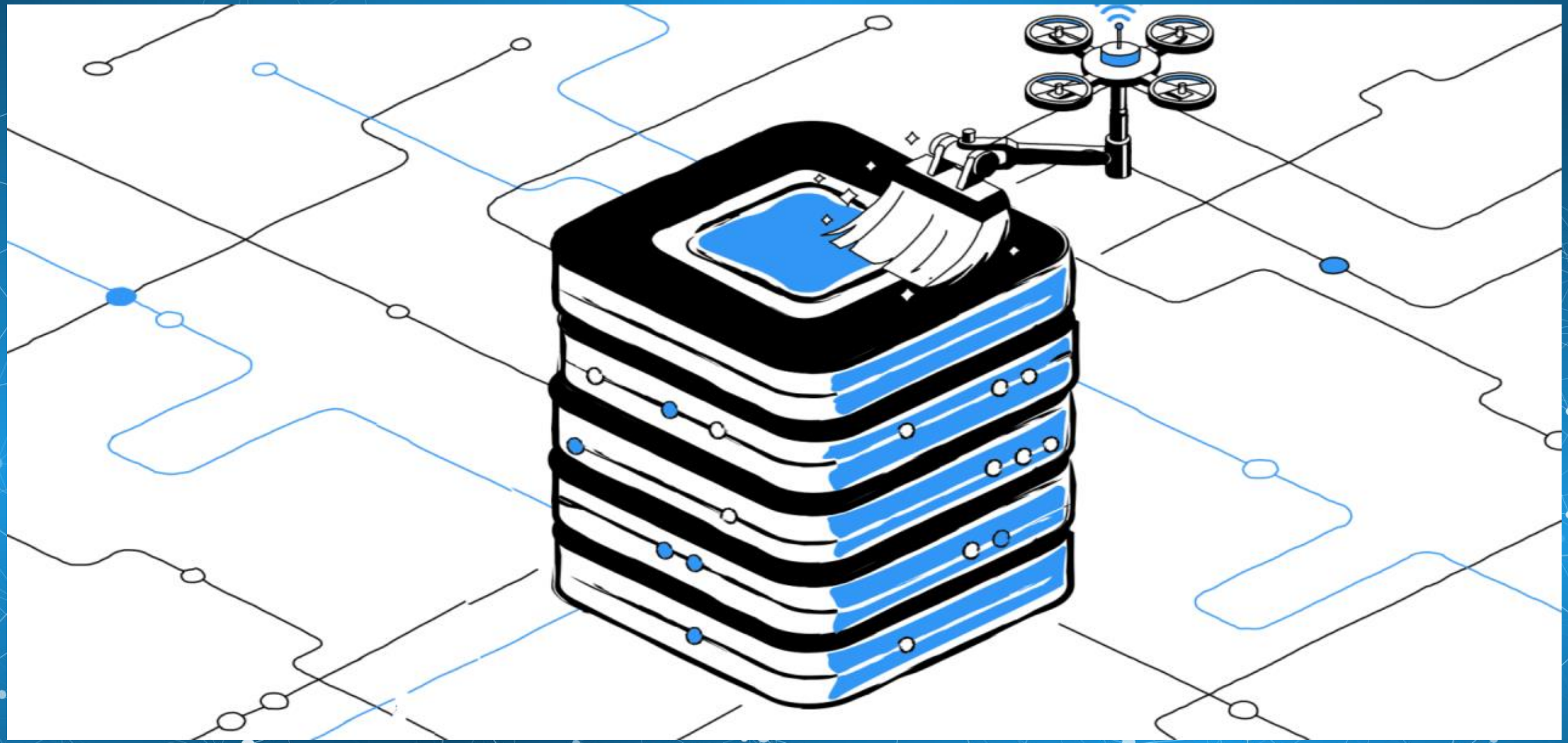
Raccolta di dati ottenuti tramite un gioco pubblicato nel Google Play Store ed Apple AppStore.

- gioco di brainstorming che mira ad acquisire, dati da:
  - Touchscreen;
  - Accelerometro;
  - Giroscopio;
  - Magnetometro;
- simula il normale utilizzo di uno smartphone:
  - tap;
  - swipe orizzontali;
  - swipe verticali;
- Si compone di diversi minigames:
  - Tipologia di giochi:
    - Focus:
    - Mathisis;
    - Memoria;
    - Reacton;
    - Speedy.
  - Più di 2000 utenti;
  - 10 Hz;
  - ambiente non controllato.

Dataset: HMOG

- Dataset che mira a raccogliere dati da:
  - Touch screen;
  - Accelerometro;
  - Giroscopio;
  - Magnetometro;
- 3 ore di partecipazione media per utente;
- simulando le più comuni attività svolte durante l'utilizzo dello smartphone;

- Attività:
  - lettura;
  - scrittura;
  - navigazione mappa.
- Modalità:
  - in camminata;
  - stando seduti.
- 100 utenti;
- 100 Hz;
- ambiente controllato.



Preprocessing

ISLab Intelligent Systems Laboratory

Preprocessing

BrainRun

- Rimozione utenti senza letture;
- Bilanciamento dei dati per utente;
- Up-sampling/Down-sampling per equalizzare la frequenza di campionamento;
- Rimozione outliers.

HMOG

- Rimozione utenti senza letture;
- Rimozione utenti che hanno svolto le attività con lo smartphone in orizzontale;
- Rimozione outliers.

Preprocessing

Rimozione utenti senza letture: sia in BrainRun che in HMOG alcuni utenti mancavano di letture di accelerometro o giroscopio o entrambe:

- 239 per BrainRun;
- 4 per HMOG.

Preprocessing (BrainRun)

Complicazioni:

1. diversa frequenza di gioco;
2. diverse frequenze di campionamento.

Per ovviare a questi problemi:

1. Bilanciamento dei dati per utente: in media ogni utente ha 71 file di dati:
   - Rimozione degli utenti che hanno meno di 71 file;
   - resampling dei file per gli utenti che ne hanno più di 71;
     - 158 utenti rimanenti.
2. Up-sampling/Down-sampling:
   - Ogni file contiene circa 1 minuto di gioco: 10 Hz = 10 letture/secondo = 600 letture/minuto
     - Up-sampling per i file con #letture < 600 (interpolazione lineare)
     - Down-sampling per i file con #letture > 600 (down-sampling factor)

Preprocessing (HMOG)

Un ristretto numero di utenti hanno svolto alcuni task con lo smartphone in modalità orizzontale e si è deciso di rimuoverli;

- 76 utenti rimanenti.

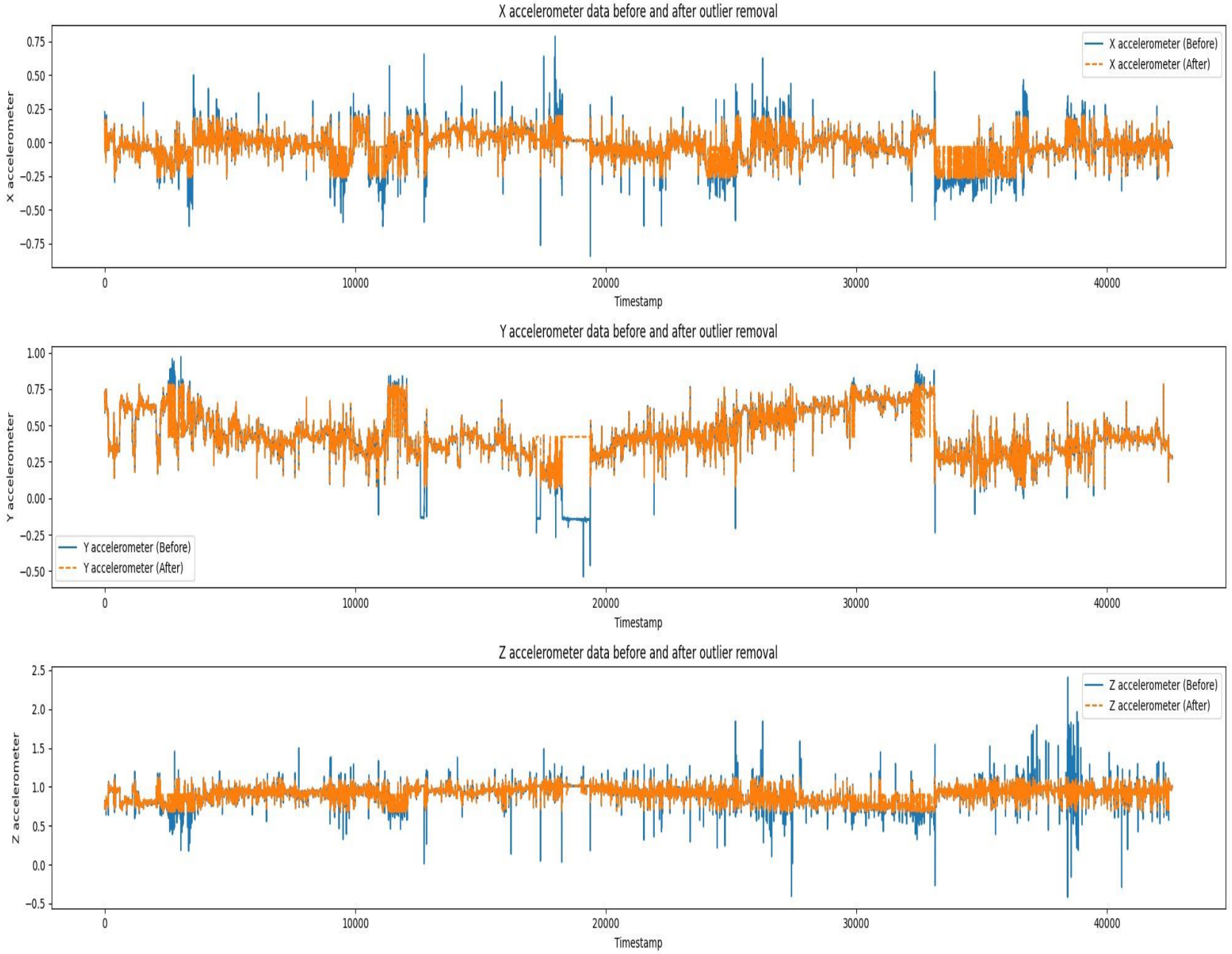
Preprocessing

Si è scelto di utilizzare i dati in due modalità:

- senza la rimozione degli outliers;
- con la rimozione degli outliers -> z-score:

Preprocessing

- Calcolo dello z-score per ogni valore in ogni asse (x, y, z);
- Se z > 3 -> outlier
- Gli outlier vengono rimpiazzati con la media



Estrazione delle features

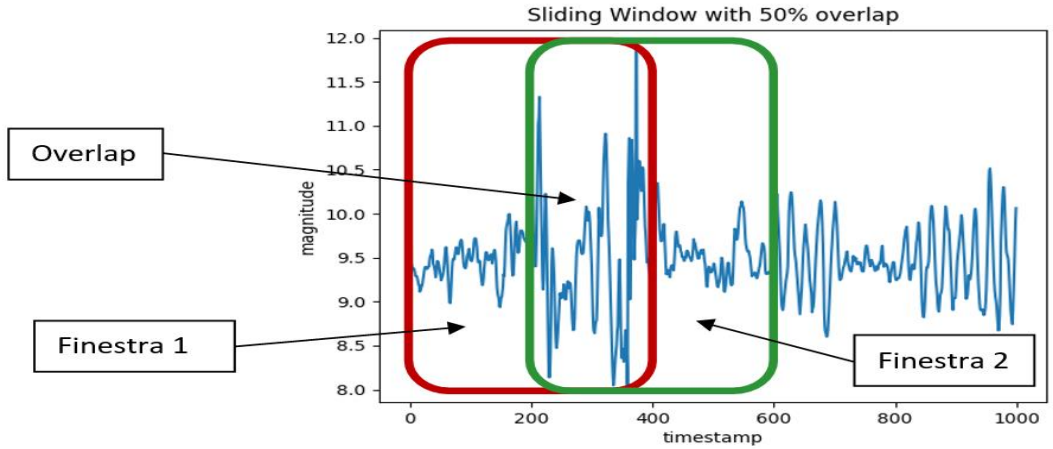
ISLab Intelligent Systems Laboratory

Estrazione delle features e normalizzazione

Per ridurre il costo computazionale e spaziale si è scelto di:

- evitare i dati di magnetometro;
- utilizzare la magnitudo del segnale $M = \sqrt{(x^2 + y^2 + z^2)}$.

Estrazione delle features tramite sliding window con 50% overlap.

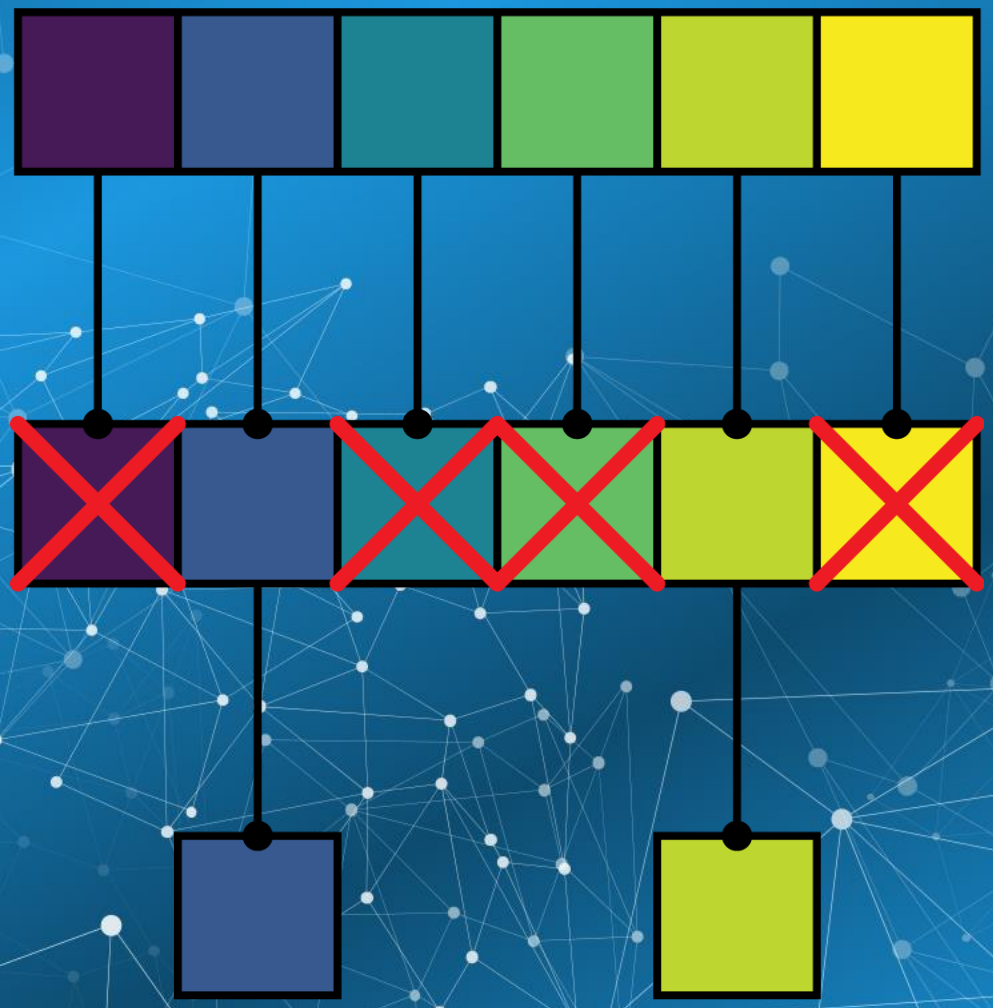


Estrazione delle features e normalizzazione

Da ogni sensore sono state calcolate:

- 23 features temporali;
- 11 features di frequenza;
- per un totale di:
  - 34 features per sensore;
  - 68 features in totale.

Applicazione Min-Max normalization -> [0, 1].



Selezione delle Features

ISLab Intelligent Systems Laboratory

Selezione delle features

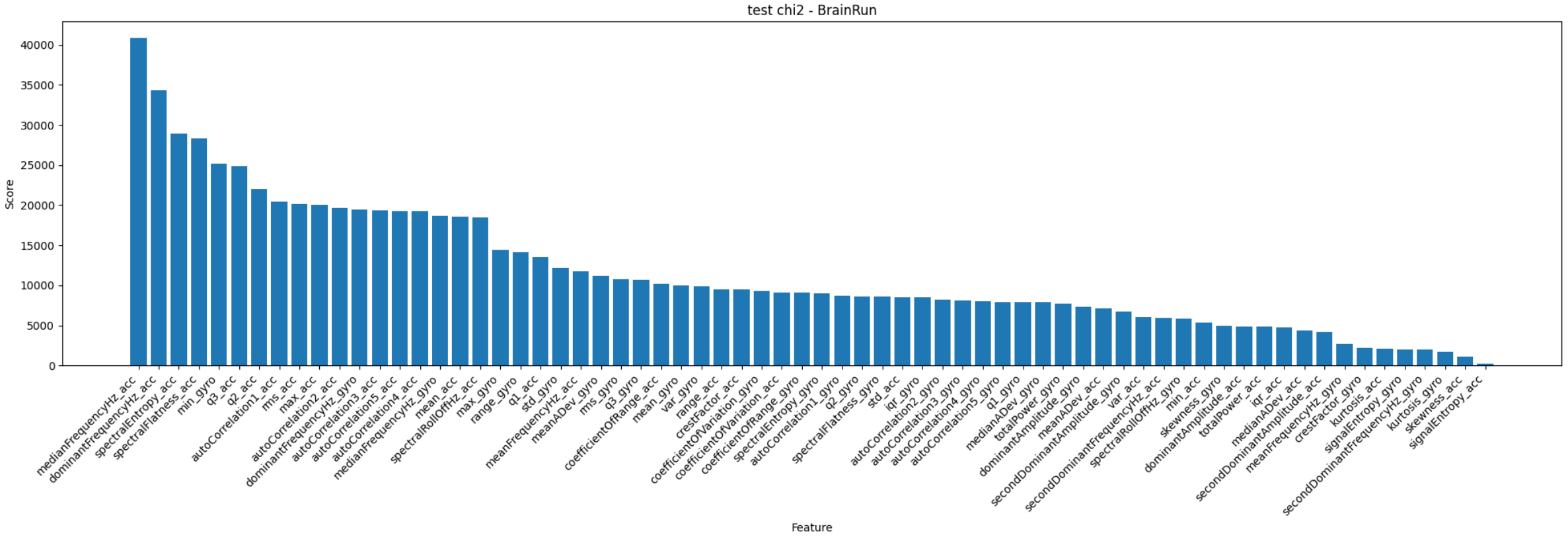
Test del X^2;

- il numero delle features non è univoco, cambia in base all'algoritmo di machine learning utilizzato.

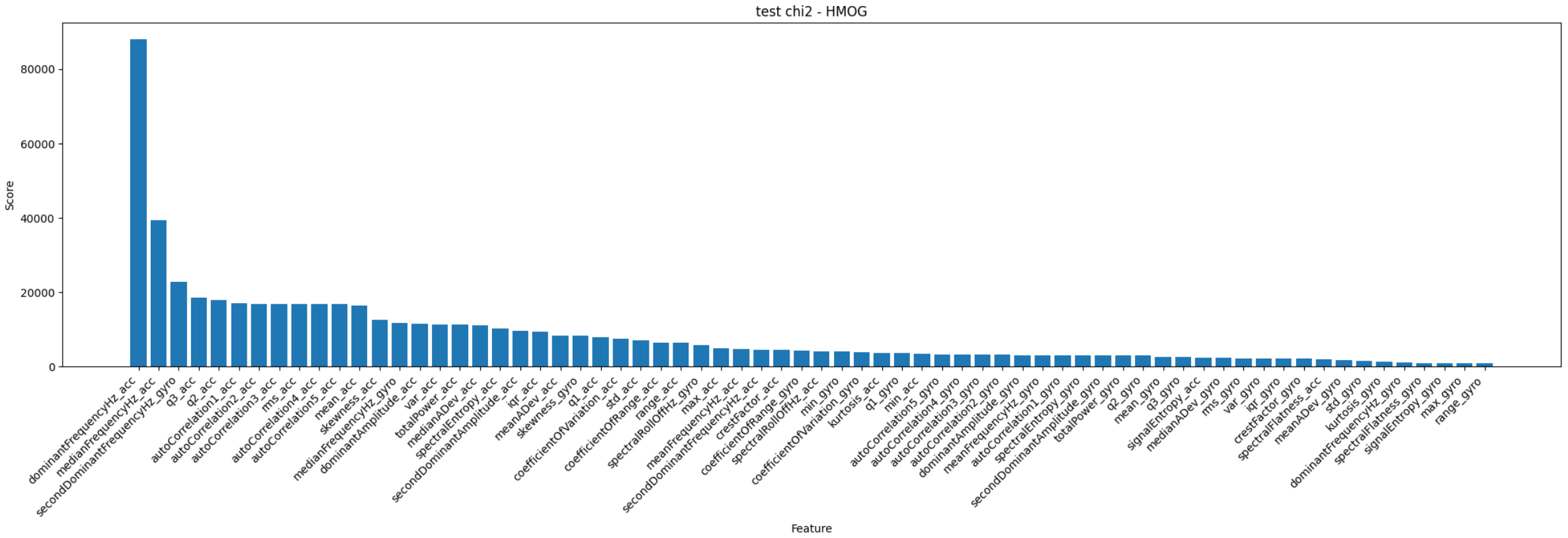
Nonostante ciò vi sono però alcune features che prendono posto in tutti (o quasi) gli algoritmi tra cui:

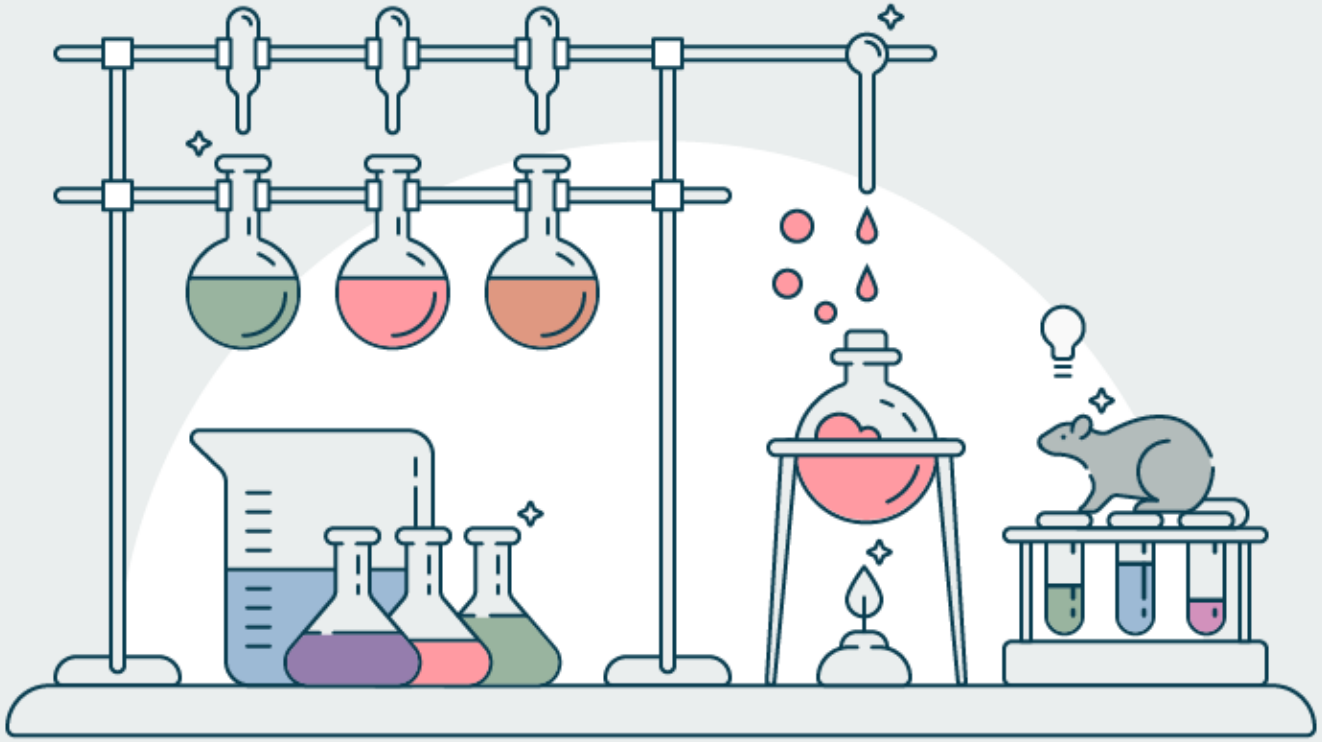
- Radice quadratica media (accelerometro)
- Coefficiente di auto correlazione (accelerometro e giroscopio)
- L'ampiezza della frequenza dominante (accelerometro e giroscopio)
- Etc.

Selezione delle features con test del chi quadro (BrainRun dataset)



Selezione delle features con test del chi quadro (HMOG dataset)





Sperimentazione

ISLab Intelligent Systems Laboratory

Sperimentazione

Per trovare la più efficiente combinazione di iperparametri si è utilizzato un sottoinsieme composto da:

- 20 utenti;
- 25 feature estratte da BrainRun per un tempo di autenticazione pari a 5 secondi, senza la rimozione degli outliers;

Dopo aver impostato i migliori iperparametri:

- incremento del numero di features;
- utilizzo di features ottenute con la rimozione degli outliers
- tecnica del K-Fold (k = 10).

Sperimentazione: One-Class SVM (OCSVM)

- kernel gaussiano;
- nu = 0.2;
- 60 features;
- senza rimozione degli outliers.

Sperimentazione: Isolation Forest (IF)

- 100 sottoalberi;
- contamination = 0.25;
- 60 features;
- con rimozione degli outliers.

Sperimentazione: Elliptic Envelope (EE)

- contamination = 0.1;
- 60 features;
- senza rimozione degli outliers.

Sperimentazione:
Osservazione sugli algoritmi One-Class

	FAR	FRR
OC-SVM	10.7%	20.10%
IF	8%	25.3%
EE	4.6%	10%

Sperimentazione: Random Forest (RF)

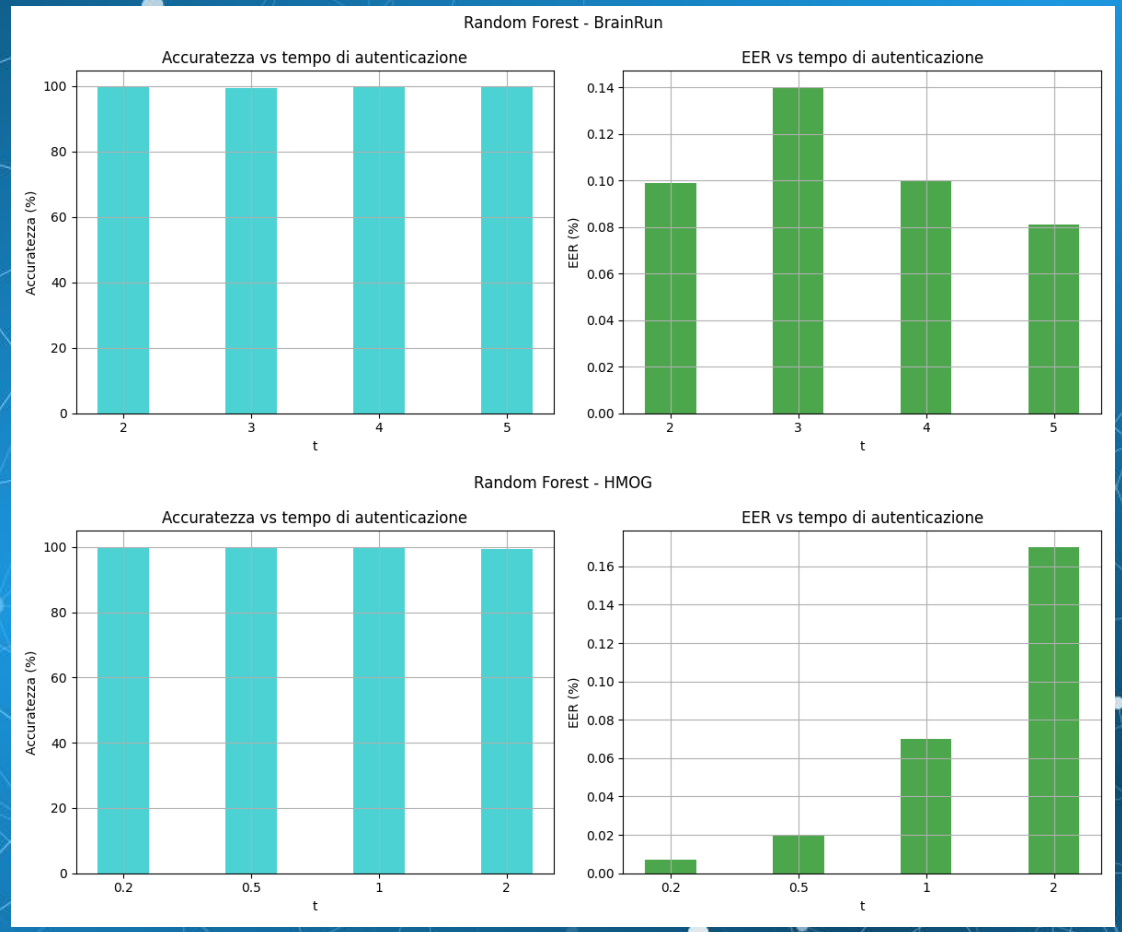
- 60 sottoalberi;
- 40 features;
- senza rimozione degli outliers.

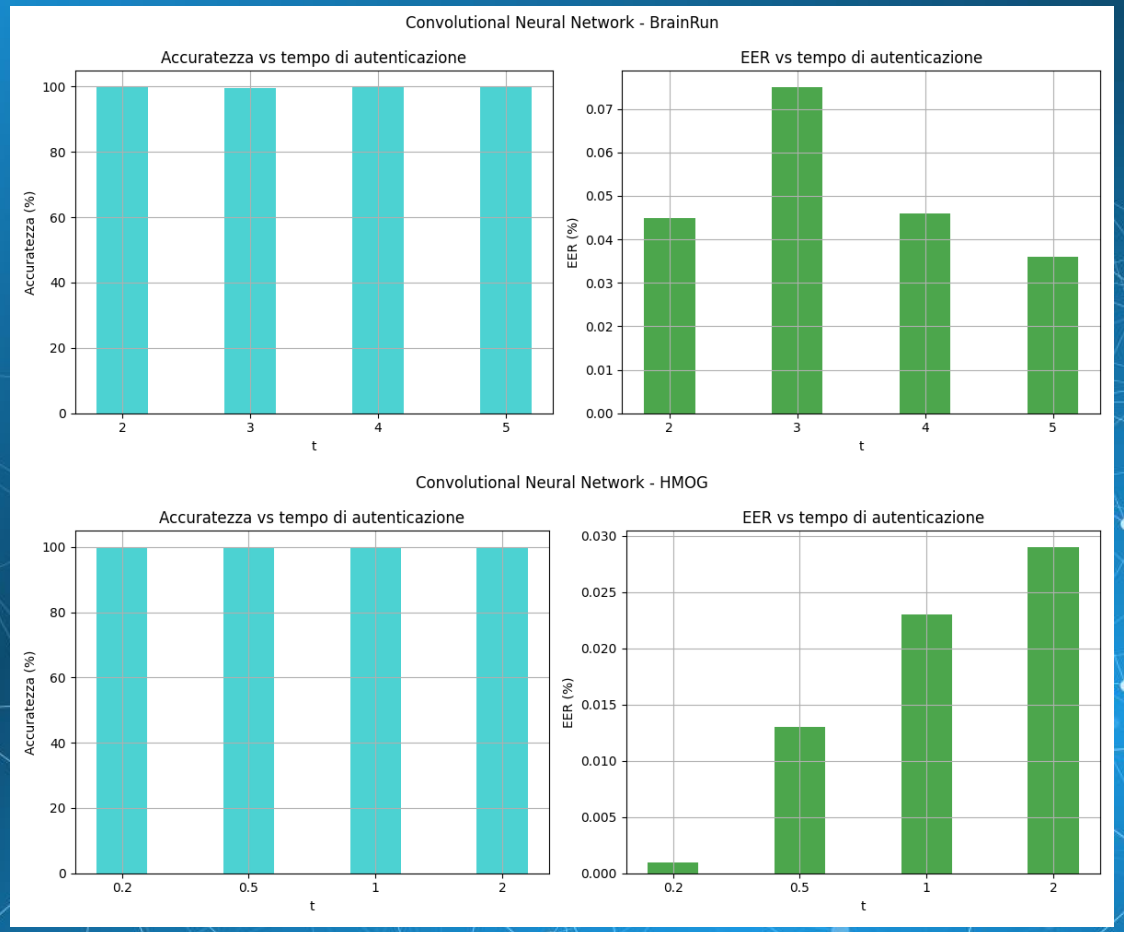
Sperimentazione: Convolutional Neural Network 1D (CNN)

- 40 features;
- senza la rimozione degli outliers.

Risultati

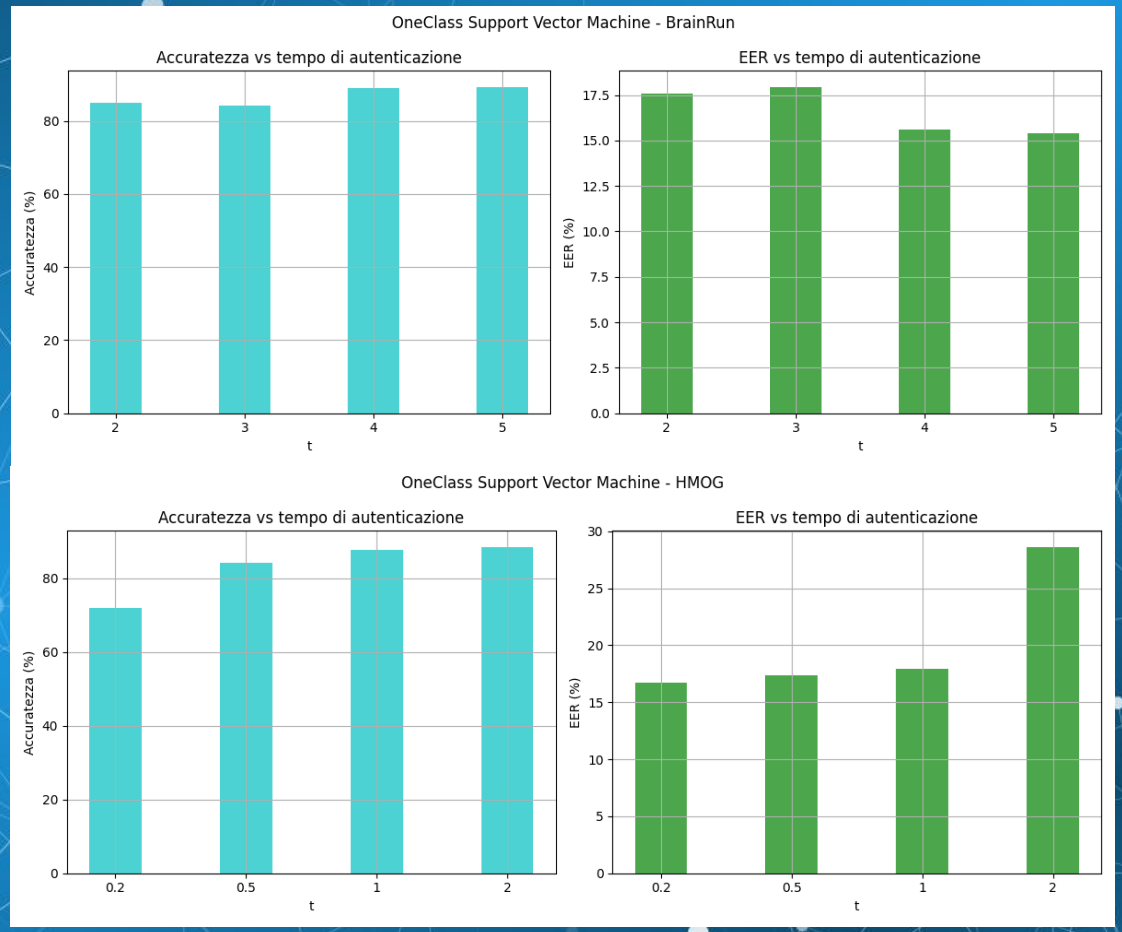
ISLab Intelligent Systems Laboratory

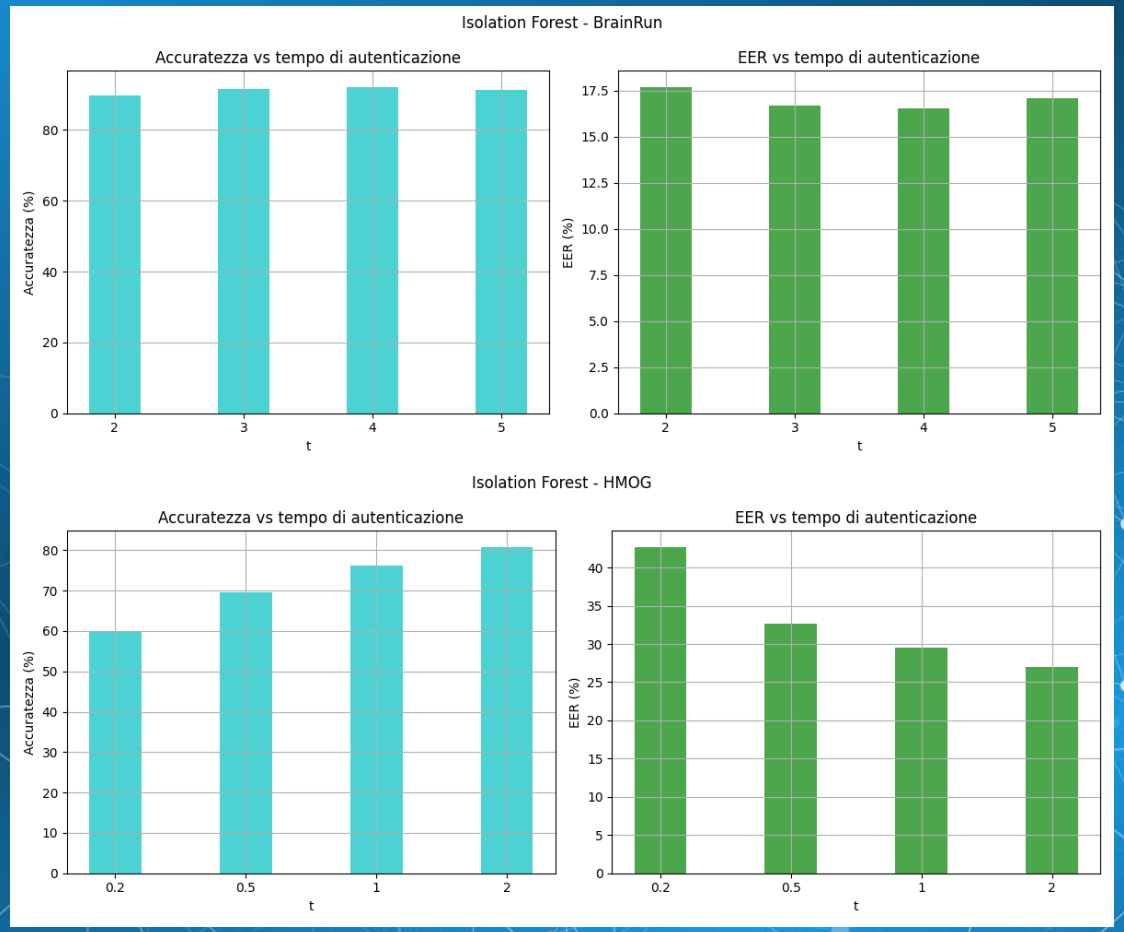




Risultati

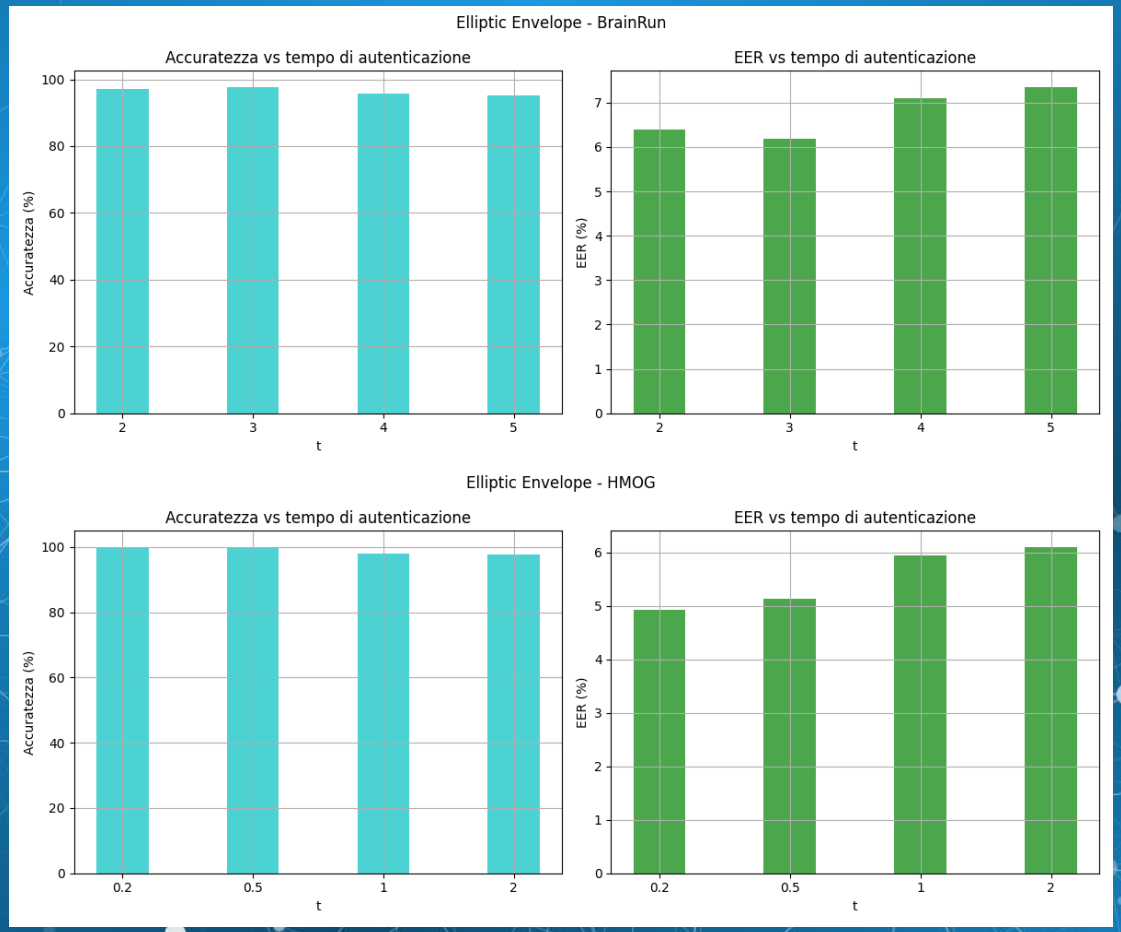
ISLab Intelligent Systems Laboratory





Risultati

ISLab Intelligent Systems Laboratory



Risultati

ISLab Intelligent Systems Laboratory

Accuratezza	BrainRun				HMOG			
tempo	2 s	3 s	4 s	5 s	0.2 s	0.5 s	1 s	2 s
RF	99.68%	99.53%	99.60%	99.64%	99.97%	99.91%	99.79%	99.48%
CNN	99.79%	99.65%	99.67%	99.76%	99.96%	99.95%	99.90%	99.84%
OC-SVM	84,9%	84.12%	88.9%	89.22%	88.48%	87.69%	84.19%	72%
IF	89.68%	91.63%	92.13%	91.21%	59.79%	69.54%	76.1%	80.75%
EE	97.1%	97.65%	95.8%	95.34%	99.96%	99.93%	98.1%	97.76%

Accuratezza	BrainRun	HMOG
tempo	2s	2s
RF	**99.68%**	99.48%
CNN	99.79%	**99.84%**
OC-SVM	**84,9%**	72%
IF	**89.68%**	80.75%
EE	97.1%	**97.76%**

EER	BrainRun				HMOG			
tempo	2 s	3 s	4 s	5 s	0.2 s	0.5 s	1 s	2 s
RF	0.09%	0.14%	0.1%	0.08%	0.01%	0.02%	0.07%	0.17%
CNN	0.04%	0.07%	0.05%	0.04%	0.01%	0.01%	0.03%	0.03%
OC-SVM	17.56%	17.93%	15.58%	15.42%	16.74%	17.37%	17.9%	28.6%
IF	17.69%	16.69%	16.52%	17%	42.67%	32.75%	29.47%	27.16%
EE	6.44%	6.18%	7.12%	7.35%	5%	5%	5.9%	6.1%

EER	BrainRun	HMOG
tempo	2 s	2 s
RF	**0.09%**	0.17%
CNN	0.04%	**0.03%**
OC-SVM	**17.56%**	28.6%
IF	**17.69%**	27.16%
EE	6.44%	**6.1%**

Risultati

ISLab Intelligent Systems Laboratory

Conclusioni

ISLab Intelligent Systems Laboratory

Conclusioni

Escludendo una frequenza di campionamento maggiore di 10 Hz si può affermare che:

- in un contesto personale, EE batte gli altri due algoritmi ad una classe:
  - 2-3 secondi di autenticazione;
  - 97.37 % di accuratezza;
  - 6.31 % EER;
  - 4.6 % FAR;
  - 10 % FRR;
- in un contesto militare o aziendale, CNN 1D risulta essere molto discriminante:
  - 2 secondi di autenticazione;
  - 99.79 % accuratezza;
  - 0.04 % EER.

Sviluppi futuri

ISLab Intelligent Systems Laboratory

Sviluppi futuri

- Integrare con Touch Dynamics;
- Integrare con Gait recognition;
- Riconoscere, oltre che autenticare, possibili patologie dell'utente in base ai tremori della mano o anomalie nella camminata;
- Utilizzo della biometria comportamentale tramite GPS;

Il tutto con il fine di sviluppare un sistema di autenticazione h24 in grado di riconoscere eventuali situazioni di rischio.

ISLab
Intelligent
Systems
Laboratory

GRAZIE PER L'ATTENZIONE