



TOR VERGATA

Progetto ML

Classificazione binaria di flussi di rete
per Intrusion Detection

Torroni Alessio 0365661

04/03/2025



INTRODUZIONE

OBIETTIVO

Classificare i flussi di rete in due categorie:

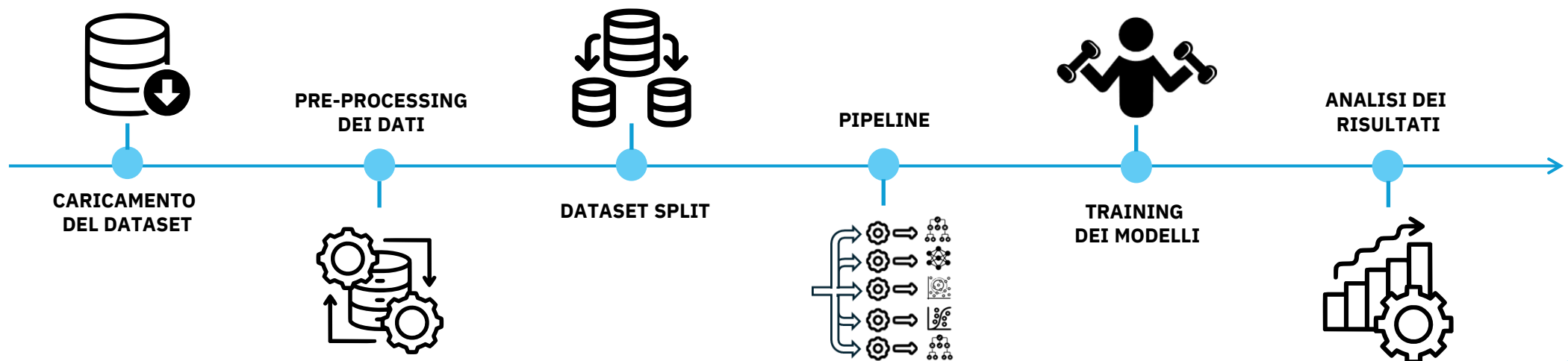
- NORMALE*
- ATTACCO*

DATASET

NSL-KDD, benchmark per sistemi di Intrusion Detection.

CARATTERISTICHE

Contiene flussi di traffico etichettati con informazioni dettagliate.





PRE-PROCESSAMENTO DEI DATI

OBIETTIVO

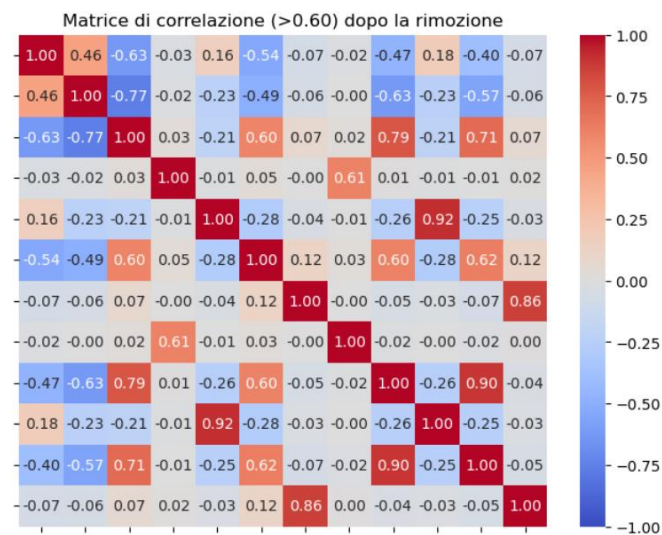
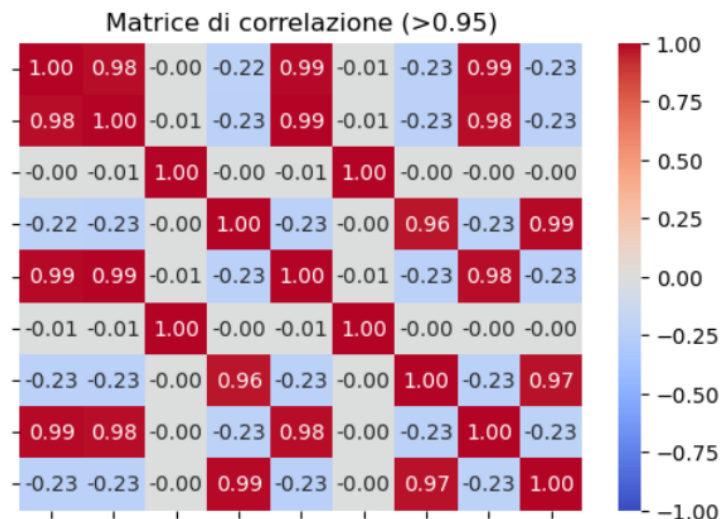
Ottimizzare il dataset, migliorando velocità e stabilità dei modelli

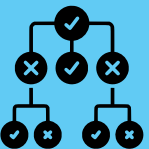
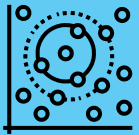
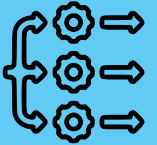
RIMOZIONE DELLE FEATURE ALTAMENTE CORRELATE

Vengono rimosse le feature con coefficiente di correlazione > 0.95

ELIMINAZIONE DELLE COLONNE A VALORI COSTANTI

Le feature a valori costanti non aggiungono variabilità ai dati





DIVISIONE DEL DATASET

DIVISIONE IN TRAINING, VALIDATION E TEST SET

Il dataset è stato diviso in: 60% training 20% validation e 20% test

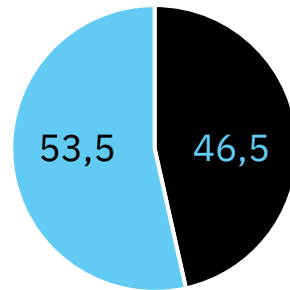
DIVISIONE DEL DATASET PRIMA DELLA NORMALIZZAZIONE

Il dataset è stato splittato prima della normalizzazione per evitare il *Data Leakage*

CONTROLLO DELLA DISTRIBUZIONE DELLE CLASSI

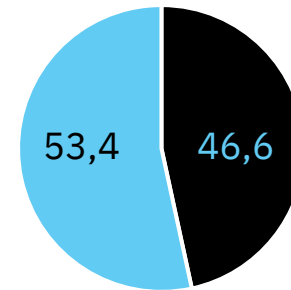
Viene controllato se le due classi sono bilanciate

Training set



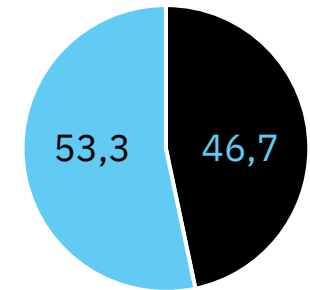
■ Attacco ■ Normale

Validation set



■ Attacco ■ Normale

Test set



■ Attacco ■ Normale



MOTIVO DELLA SCELTA

Consente di suddividere il pre-processing in fasi distinte, adattando le trasformazioni alle diverse tipologie di feature secondo il modello.

NORMALIZZAZIONE DELLE FEATURE NUMERICHE

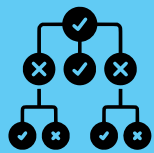
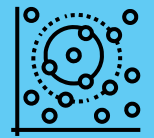
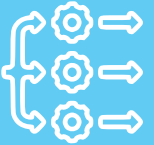
Le feature numeriche vengono normalizzate utilizzando *MinMaxScaler*

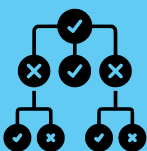
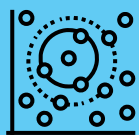
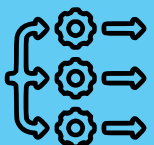
ENCODING DELLE FEATURE CATEGORICHE

- Feature a bassa dimensionalità:  *One Hot Encoding*
- Feature ad alta dimensionalità:  *Target Encoding*

NORMALIZZAZIONE DIVERSA IN BASE AL MODELLO

- Modelli *sensibili* alle scale: tutte le feature vengono normalizzate
- Modelli *NON sensibili* alle scale: vengono normalizzate solo le feature categoriche e le feature numeriche a valori troppo elevati





NEURAL NETWORK

ARCHITETTURA

- 2 Hidden Layers
- Funzione di attivazione *ReLU* per gli hidden layers e *sigmoid* per l'output layer
- Dropout e Early Stopping per ridurre il rischio di overfitting

OTTIMIZZAZIONE DEGLI IPERPARAMETRI

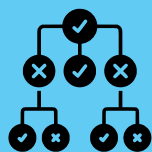
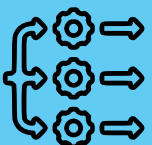
Ricerca dei migliori parametri attraverso *RandomizedSearchCV*

PRESTAZIONI DEL MODELLO

METRIC	VALUE
Accuracy	0.995594
Precision	0.995594
Recall	0.995594
F1-Score	0.995594

Confusion Matrix

Actual	Normal	Attack
Normal	13413	53
Attack	58	11671
	Normal	Attack
	Predicted	



K-NEAREST NEIGHBORS

ARCHITETTURA

- Numero di vicini $k=4$
- Tipo di peso dei vicini è determinato dalla *distanza*
- Metrica di distanza *Manhattan*

OTTIMIZZAZIONE DEGLI IPERPARAMETRI

Ricerca dei parametri è avvenuta attraverso *RandomizedSearchCV*

PRESTAZIONI DEL MODELLO

METRIC	VALUE
Accuracy	0.996706
Precision	0.996706
Recall	0.996706
F1-Score	0.996706

Confusion Matrix

Actual	Normal	Attack
Normal	13426	40
Attack	43	11686
	Normal	Attack
	Predicted	



LOGISTIC REGRESSION

REGOLARIZZAZIONE

Viene effettuata una regolarizzazione L2 con parametro C ottimizzato

OTTIMIZZAZIONE DEGLI IPERPARAMETRI

Ricerca dei parametri è avvenuta attraverso *GridSearchCV*

LATI NEGATIVI

Numero elevato di Falsi Negativi, buoni risultati ma è il modello meno performante

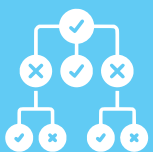
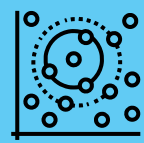
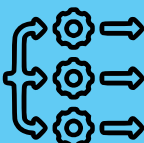
PRESTAZIONI DEL MODELLO

METRIC	VALUE
Accuracy	0.972653
Precision	0.972771
Recall	0.972653
F1-Score	0.972634

Confusion Matrix

Actual	Normal	Attack
	13234	232
Attack	457	11272
	Normal	Attack

Predicted



RANDOM FOREST

ARCHITETTURA

- 100 alberi decisionali
- La profondità massima è 20 livelli
- Il criterio di suddivisione scelto è *Gini*

OTTIMIZZAZIONE DEGLI IPERPARAMETRI

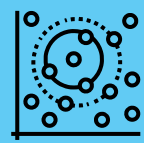
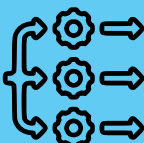
Ricerca dei migliori parametri attraverso *HalvingSearchCV*

PRESTAZIONI DEL MODELLO

METRIC	VALUE
Accuracy	0.998651
Precision	0.998652
Recall	0.998651
F1-Score	0.998650

Confusion Matrix

Actual	Normal	Attack
	13460	6
Predicted	28	11701
	Normal	Attack



ARCHITETTURA

- Boosting sequenziale: ogni nuovo albero corregge gli errori dei modelli precedenti.
- Base estimator: *Decision Trees* con $max_depth=1$
- Learning rate = 1.0

OTTIMIZZAZIONE DEGLI IPERPARAMETRI

Ricerca dei migliori parametri attraverso *GridSearchCV*

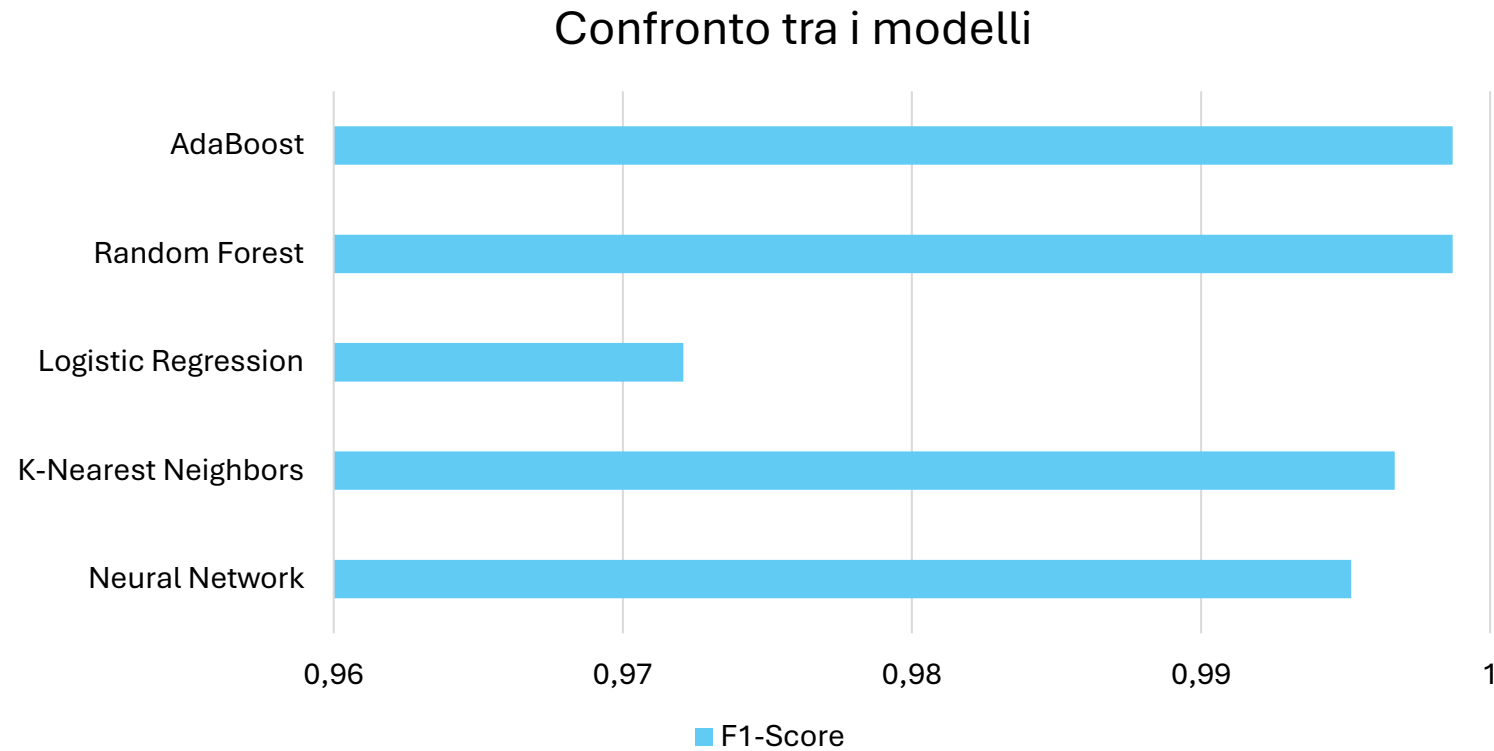
PRESTAZIONI DEL MODELLO

METRIC	VALUE
Accuracy	0.998611
Precision	0.998611
Recall	0.998611
F1-Score	0.998611

Confusion Matrix

	Actual	Normal	Attack
		13453	13
	Predicted	22	11707
		Normal	Attack

CONCLUSIONI



CONCLUSIONI

MIGLIOR MODELLO

RANDOM FOREST

Ha dimostrato di ottenere le migliori prestazioni su tutte le metriche.

PRESTAZIONI SUL TEST SET



METRIC	VALUE
Accuracy	0.998333
Precision	0.998333
Recall	0.998333
F1-Score	0.998333

Confusion Matrix

Actual	Normal	Attack
	13410	12
Predicted	30	11743
	Normal	Attack



GRAZIE
DELL'ATTENZIONE