fime

GREYC

How Artificial Intelligence can be used for Behavioral Identification?

International Conference on CyberWorlds

Yris Brice Wandji Piugie
Joël Di Manno
Christophe Rosenberger
Christophe Charrier

Presentation to:
CyberWorlds 2021

CYBERWORLDS
28-30 September
Caen
2021
International Conference

Introduction

- ❑ Behavioral biometrics (non exhaustive)

Keystroke Dynamics

Touchscreen

Human Activity

Voice and Speech Recognition

Signature

Introduction

❑ Problematic

User identification considering their behaviors.

- How **efficient** are classical **machine learning** methods on such data?
- What about **deep learning** approaches?

Contents

Related Work

❑ Human activity

Table I: Overview of activity recognition based on classical machine learning approaches. k-NN : k-Nearest Neighbor; SVM : Support Vector Machine; RF : Random Forest; MLP : Multi-Layer Perceptron; GMM : Gaussian mixture model; KF : Kalman Filter **[9]**

Paper	Approach	Method	Activity	Input Source	Performance
[10]	Comparison study to classify human activities	SVM, MLP, RF,Naive Bayes	Sleeping, eating, walking, falling, talking on the phone	Image	86.0%
[11]	Hybrid deep learning for activity and action recognition	GMM, KF, Gated Recurrent Unit	Walking, jogging, running, boxing, hand-waving, hand-clapping	Video	96.3%
[12]	Infer high-level rules for noninvasive ambient that help to anticipate abnormal activities	RF	Abnormal activities: agitation, alteration, screams, verbal aggression, physical aggression and inappropriate behavior	Ambient sensors	98.0%
[13]	Active learning to recognize human activity using Smartwatch	RF, Extra Trees, Naive Bayes, Logistic Regression, SVM	Running, walking, standing, sitting, lying down	Smartwatch	93.3%
[14]	Recognizing human activity using smartphone sensors	Quadratic, k-NN, ANN, SVM	Walking upstairs, downstair	Smartphone	84.4%

[9] F. Al Machot, M. R Elkobaisi, and K. Kyamakya, “Zero-shot human activity recognition using non-visual sensors,” Sensors, vol. 20, no. 3, p. 825, 2020.
[10] P. M. D. Alex, A. Ravikumar, J. Selvaraj, and A. Sahayadhas, “Research on human activity identification based on image processing and artificial intelligence,” Int. J. Eng. Technol, vol. 7, 2018.
[11] N. Jaouedi, N. Boujnah, and M. S. Bouhlel, “A new hybrid deep learning model for human action recognition,” Journal of King Saud University-Computer and Information Sciences, vol. 32, no. 4, pp. 447–453, 2020.
[12] M. Á. Antón, J. Ordieres-Meré, U. Saralegui, and S. Sun, “Non-invasive ambient intelligence in real life: Dealing with noisy patterns to help older people,” Sensors, vol. 19, no. 14, p. 3113, 2019.
[13] F. Shahmohammadi, A. Hosseini, C. E. King, and M. Sarrafzadeh, “Smartwatch based activity recognition using active learning,” in 2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE). IEEE, 2017, pp. 321–329.
[14] D. Anguita, A. Ghio, L. Oneto, X. Parra, and J. L. Reyes-Ortiz, “A public domain dataset for human activity recognition using smartphones.” in Esann, vol. 3, 2013, p. 3.

Related Work

❑ Keystroke dynamics

Table II: Overview of keystroke dynamics relative works and performance metrics [19]

Study	Features	Classification	Testing type	Env.	Subjects	Samples	Identification Rate (%)
[20]	Latency, Trigraph/N-graph	Distance measure	Static, Dynamic	controlled	40	364	90
[21]	Key Pressure	Statistical classifiers	Static	Controlled	50	3000	6.6
[22]	Latency, Key hold time	Statistical	Static	Controlled	37	-	72.97
[23]	Latency	Statistical	Static	Controlled	11	-	76
[24]	Latency, Key hold time	Euclidean dist.	Static	Controlled	112	-	90.7

[20] F. Bergadano, D. Gunetti, and C. Picardi, “Identity verification through dynamic keystroke analysis,” Intelligent Data Analysis, vol. 7, no. 5, pp. 469–496, 2003.
[21] H.-R. Lv, Z.-L. Lin, W.-J. Yin, and J. Dong, “Emotion recognition based on pressure sensor keyboards,” in 2008 IEEE international conference on multimedia and expo. IEEE, 2008, pp. 1089–1092.
[22] M. Rybnik, M. Tabedzki, and K. Saeed, “A keystroke dynamics based system for user identification,” in 2008 7th computer information systems and industrial management applications. IEEE, 2008, pp. 225–230.
[23] Z. Jin, A. B. J. Teoh, T. S. Ong, and C. Tee, “Typing dynamics biometric authentication through fuzzy logic,” in 2008 International Symposium on Information Technology, vol. 3. IEEE, 2008, pp. 1–6.
[24] T. Samura and H. Nishimura, “Keystroke timing analysis for individual identification in japanese free text typing,” in 2009 ICCAS-SICE. IEEE, 2009, pp. 3166–3170.

Comparative Study

Used models for time series classification

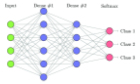
Classical Machine Learning

On Orange 3.27

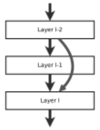
- SVM
- Neural Network
- Random Forest
- AdaBoost
- Logistic Regression
- Naive Bayes
- kNN
- Stacking

Deep Learning Models

On Python 3.8



- Fully Convolutional Neural Networks



- Residual Network

Workflow - Orange data mining software[1]

Data Mining

Open source machine learning and data visualization.

Interactive Data Visualization

Perform simple data analysis with clever data visualization.

Visual Programming

Interactive data exploration for rapid qualitative analysis with clean visualizations. It helps to build data analysis workflows visually with a large diverse toolbox

Add-ons Extend Functionality

Use various add-ons available within Orange to mine data from external data sources, perform natural language processing and text mining.

[1] https://orangedatamining.com/

Workflow

③

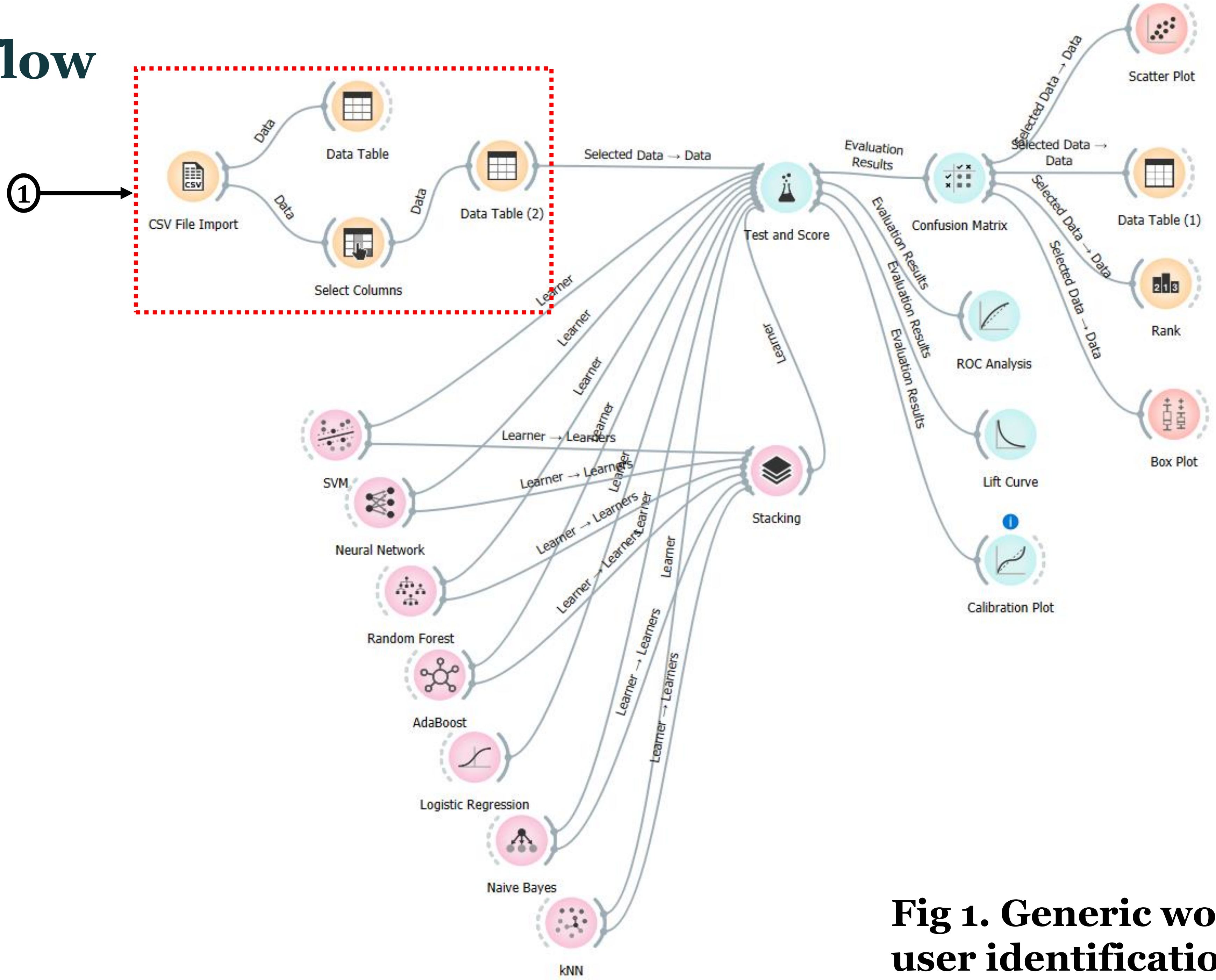


Fig 1. Generic workflow for user identification on Orange

Workflow

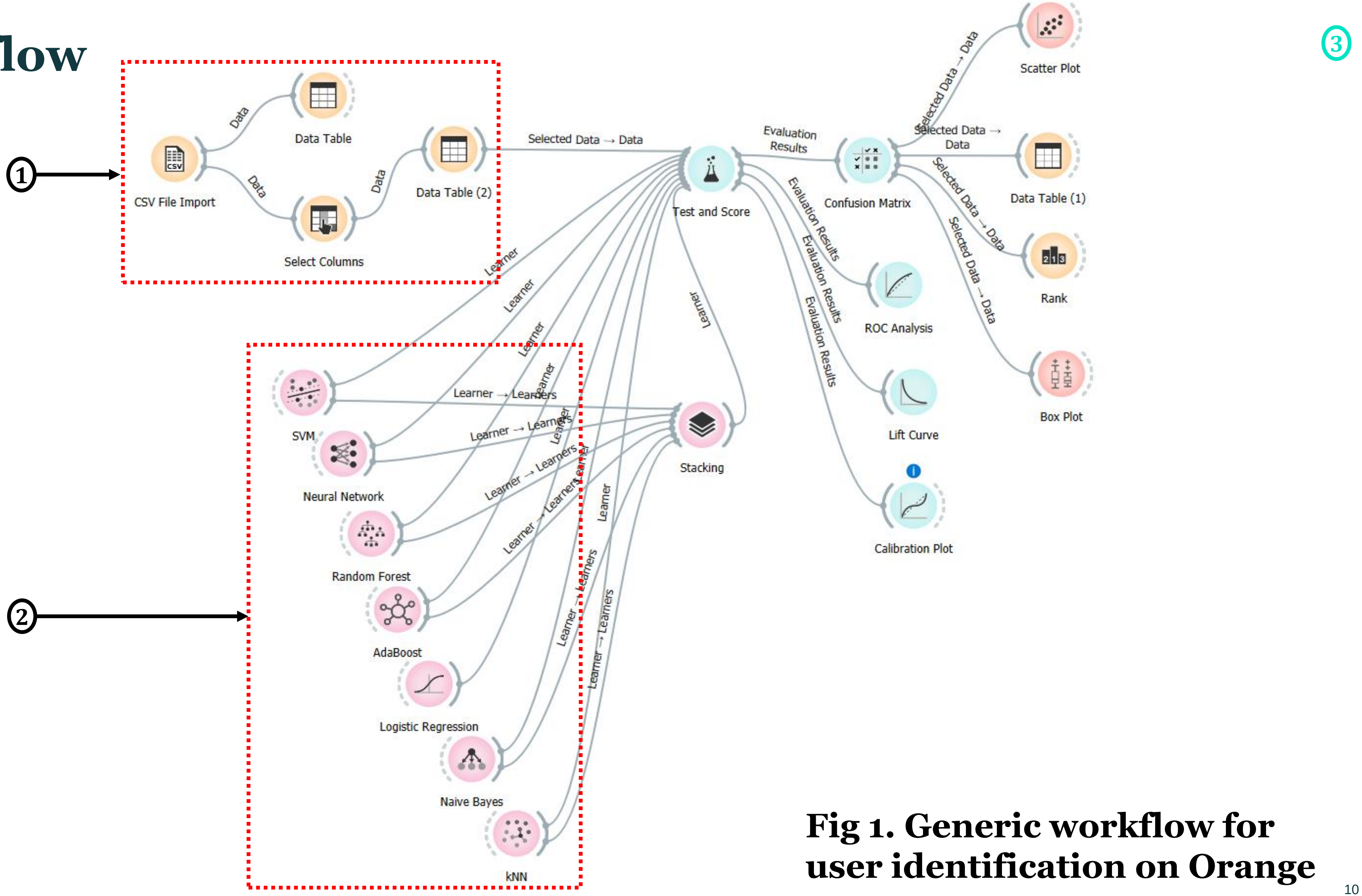


Fig 1. Generic workflow for user identification on Orange

Workflow

3

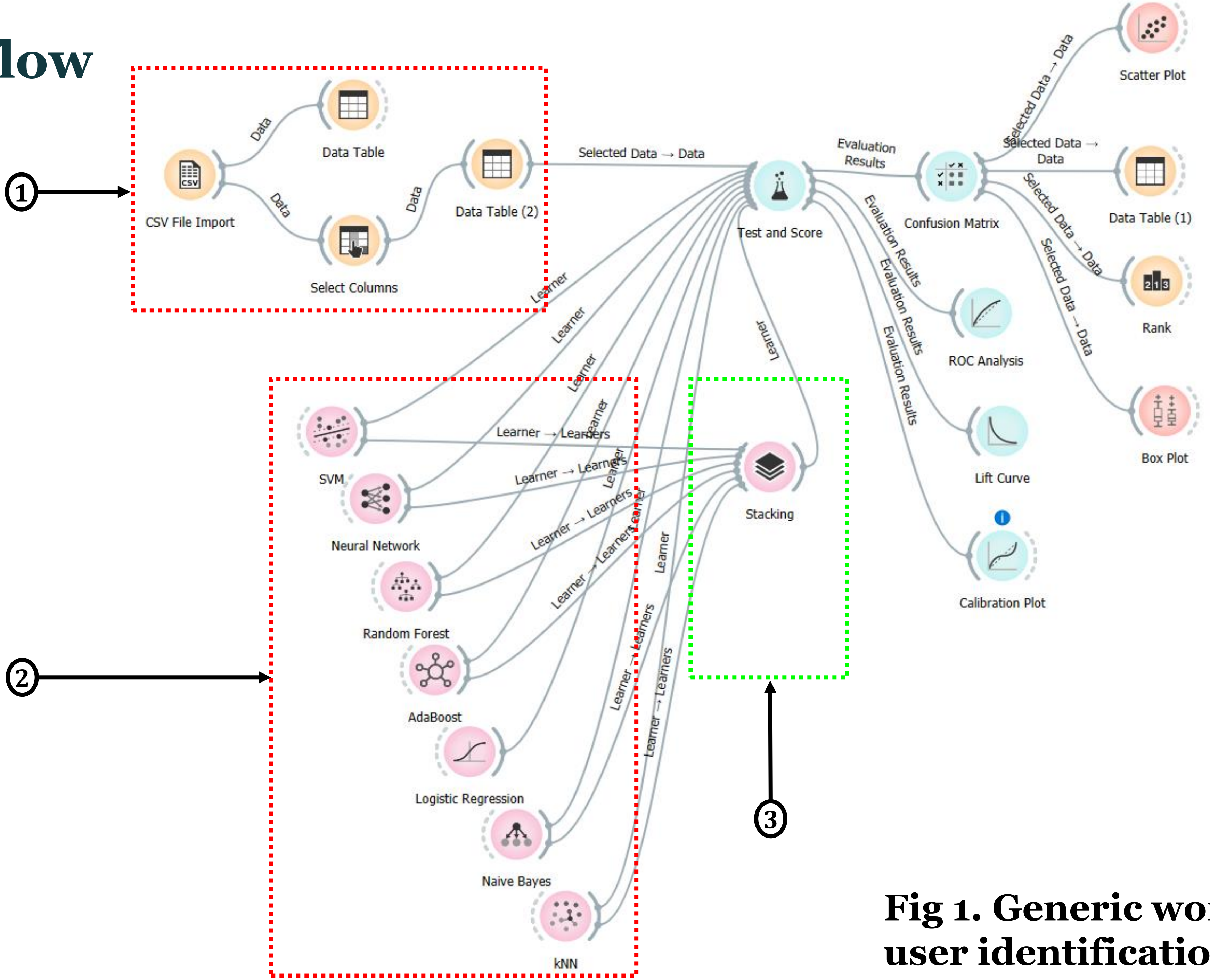


Fig 1. Generic workflow for user identification on Orange

Workflow

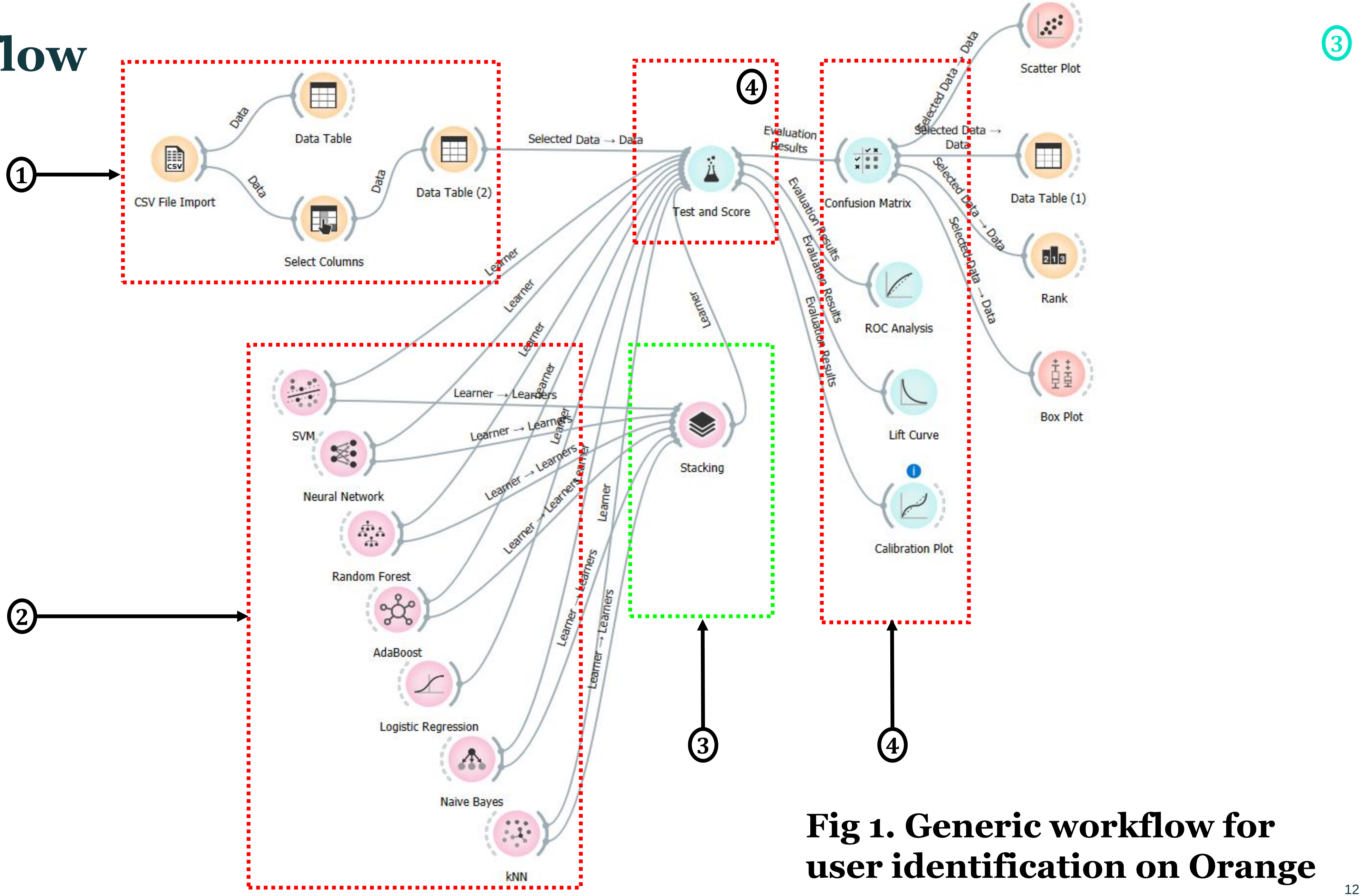


Fig 1. Generic workflow for user identification on Orange

Workflow

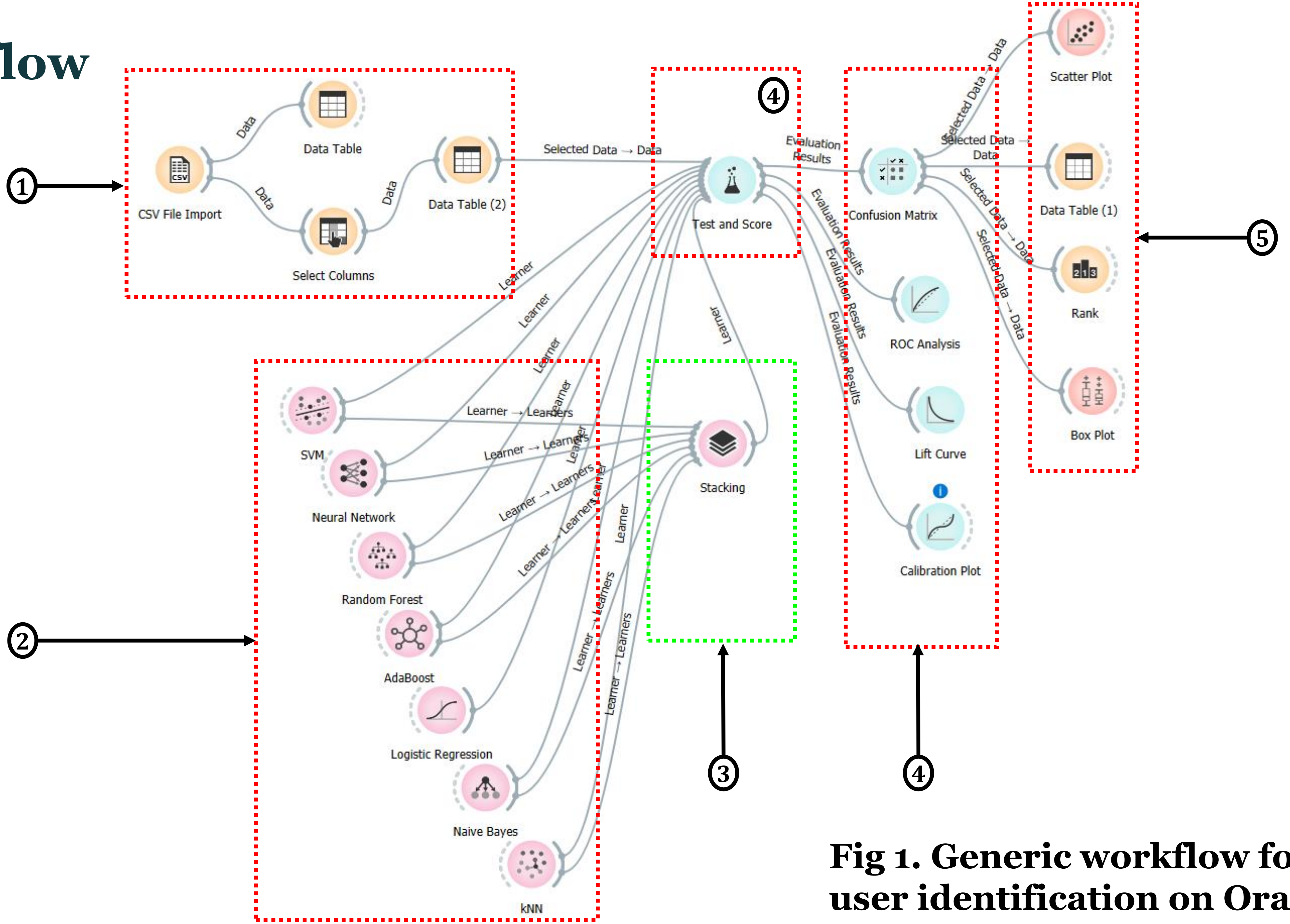
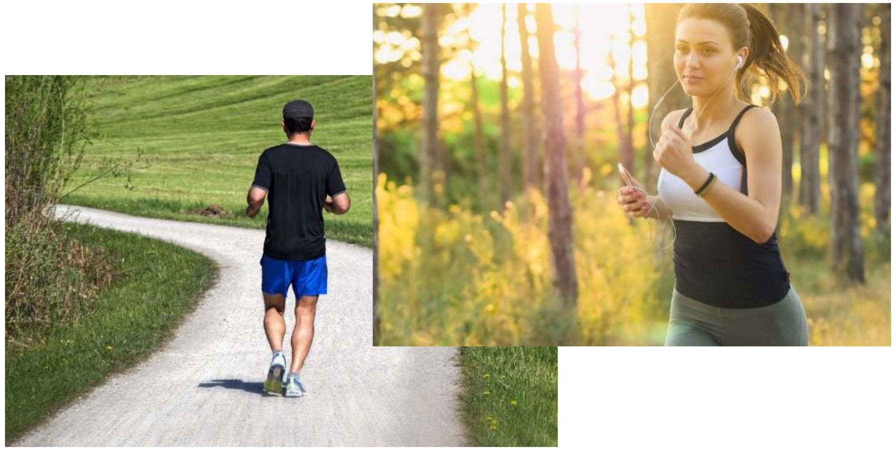


Fig 1. Generic workflow for user identification on Orange

Protocol

3

1°) Human activities – HAR database



Activities
Laying
Sitting
Standing
Walking
Walking Downstairs
Walking Upstairs

30 users

2°) Keystroke dynamics – GREYC-NISLAB database

Table III: Passphrases

Password	Description	Size	Features
P1	leonardo dicaprio	17-char	64
P2	the rolling stones	18-char	68
P3	michael schumacher	18-char	68
P4	red hot chilli peppers	22-char	84
P5	united states of america	24-char	92
P_T	fusion of features (P1+P2+P3+P4+P5)	99-char	376

110 users

Protocol

Database preprocessing

- ❑ **Training set : 70% per user data in the database**
- ❑ **Testing set : 30% per user data in the database**
- ❑ **P_T represent the fusion of features (P1+P2+P3+P4+P5) from GREYC-NISLAB database**

Performance Metrics

- Classification Accuracy (A or CA)

$$A = \frac{T_P + T_N}{T_P + T_N + F_P + F_N} \qquad (1)$$

- Precision score (P)

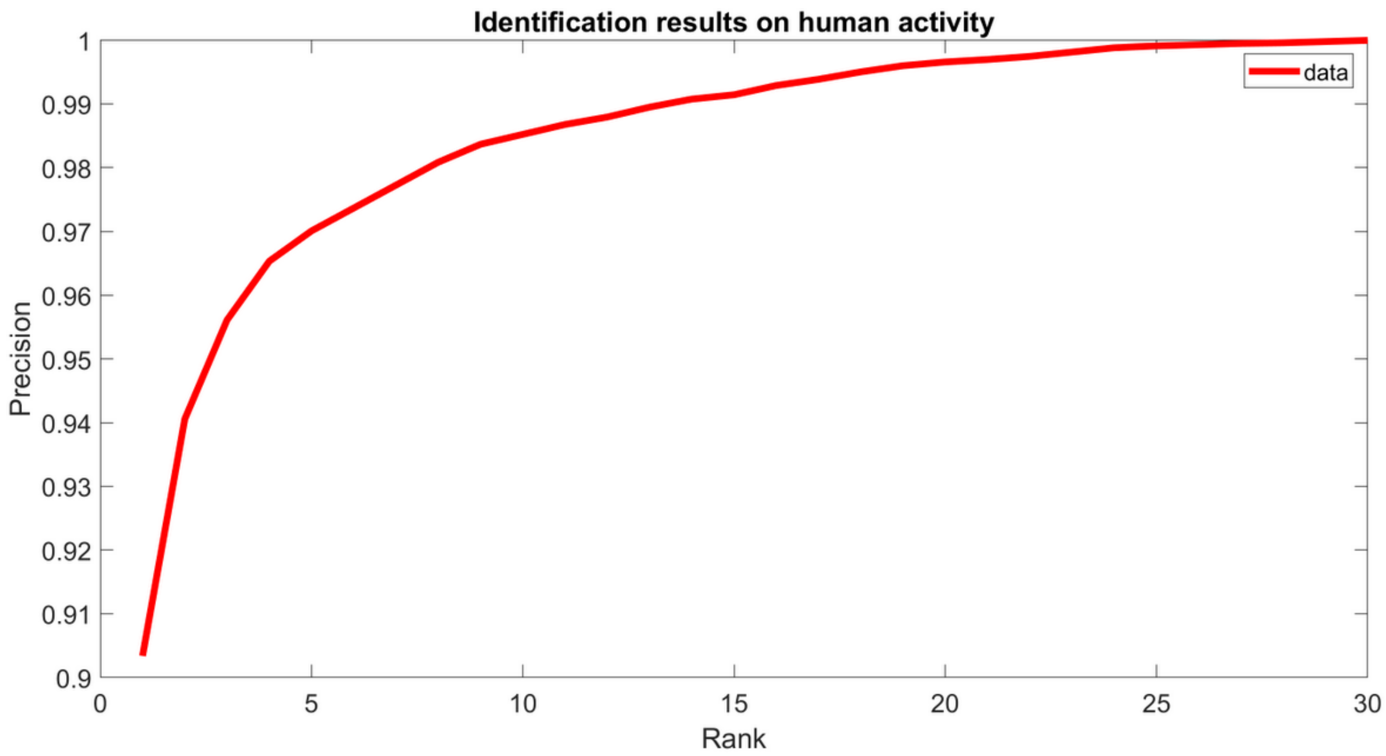
$$P = \frac{T_P}{T_P + F_P} \qquad (2)$$

- Recall (R)

$$R = \frac{T_P}{T_P + F_N} \qquad (3)$$

- Area Under the Curve (AUC)

- Cumulative Match Characteristic (CMC) Curve



Experimental Results

Performance : Deep Learning Approaches on Python 3.8

- **HAR →** UCI-HAR database
- **PT →** fusion of features (P1+P2+P3+P4+P5) from GREYC-NISLAB database

Table X: UCI-HAR and GREYC-NISLAB deep performance metrics

Dataset	Classifier name	CA (%)	P (%)	R (%)
HAR	ResNet	87.05	87.20	86.73
	FCN	68.58	80.09	68.24
P_T	ResNet	80.30	82.94	82.23
	FCN	76.06	78.95	79.01

Deep Learning Methods give good results but not exceptional !

Performance : Classical Machine Learning on Orange

❑ HAR database

Table VII: User identification performance metrics with Orange workflow on HAR dataset from human activities.

Model	AUC (%)	CA (%)	P (%)	R (%)
Stack	99.65	93.89	93.90	93.89
Neural Networks	98.97	87.75	87.73	87.75
Random Forest	98.21	85.78	85.89	85.78
kNN	97.56	81.40	82.07	81.40
AdaBoost	89.33	81.06	81.25	81.06
SVM	96.57	78.45	80.22	78.45
Logistic Regression	96.76	78.38	78.40	78.38
Naive Bayes	79.24	41.33	48.49	41.33

By analyzing users activities, and merging all the models, in **93.90%** of the cases we can recognize a person among the 30 users.

❑ GREYC-NISLAB database

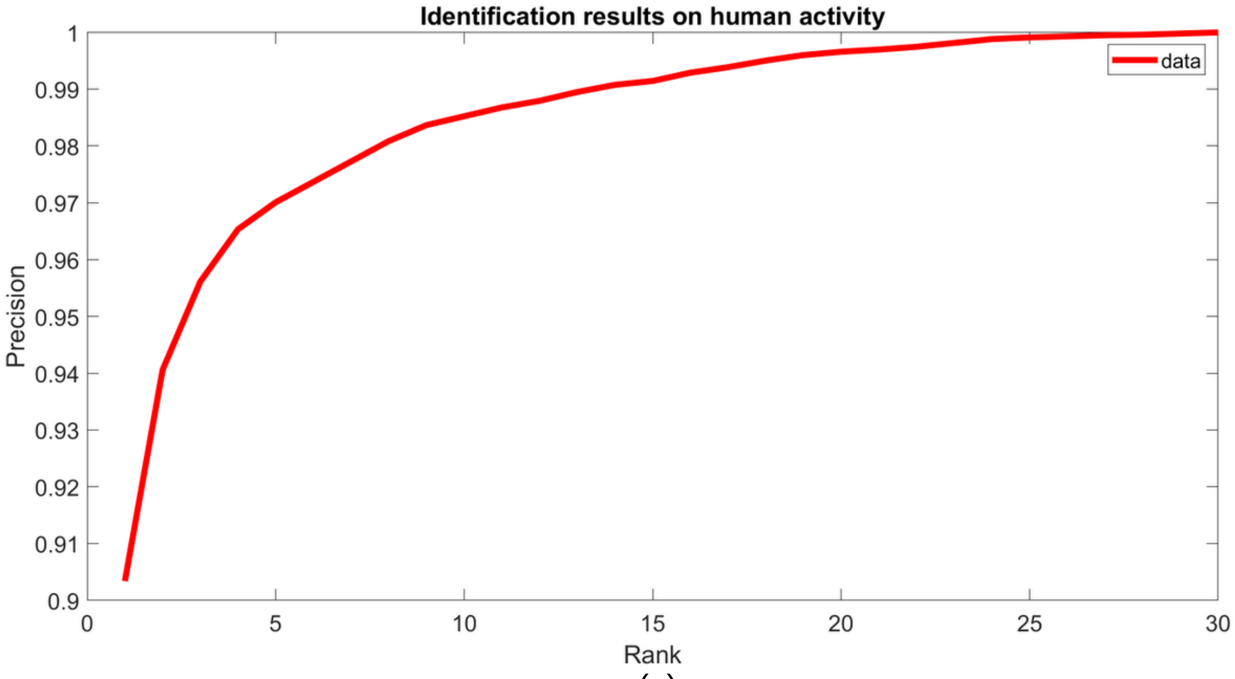
Table VIII: User identification performance metrics with Orange workflow on GREYC-NISLAB from keystroke dynamics.

Password database	Model	AUC (%)	CA (%)	P (%)	R (%)
P1	Stack	96.22	63.09	63.67	63.10
P2	Stack	99.08	69.73	72.15	69.73
P3	Stack	98.49	63.91	66.10	63.91
P4	Stack	99.22	77.73	79.64	77.73
P5	Stack	98.56	83.73	84.30	83.73
P_T	Stack	99.99	98.10	98.3	98.10

- In a context of **one type password**, **Identification rate is [63.67% - 84.30%]**
- In a context of **5 type passwords**, **Identification rate is 98.30%**

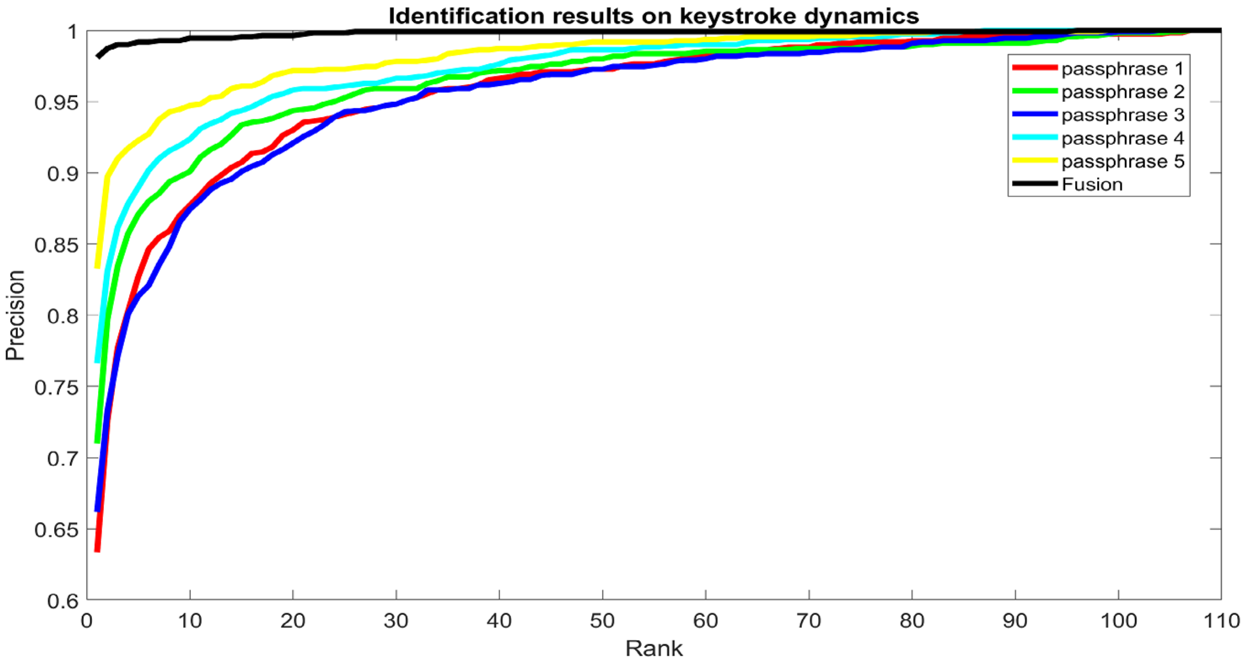
CMC curve on behavioral biometrics data

❑ HAR database



(a)

❑ GREYC-NISLAB database



(b)

Fig 4. CMC curve of Stacking model in Orange workflow

Soft biometrics

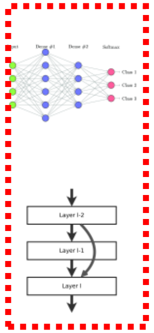
❑ Are we able to profile an user ?

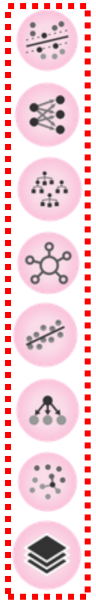
Table IX: User identification (based on user knowledge) performance with Orange workflow on GREYC-NISLAB database.

Targets	CA(%)
Subject	98.18
Handedness	99.27
Gender	88.73
Age	70.73

Traditional machine learning tools can have a significant impact on a person's privacy!

Conclusion

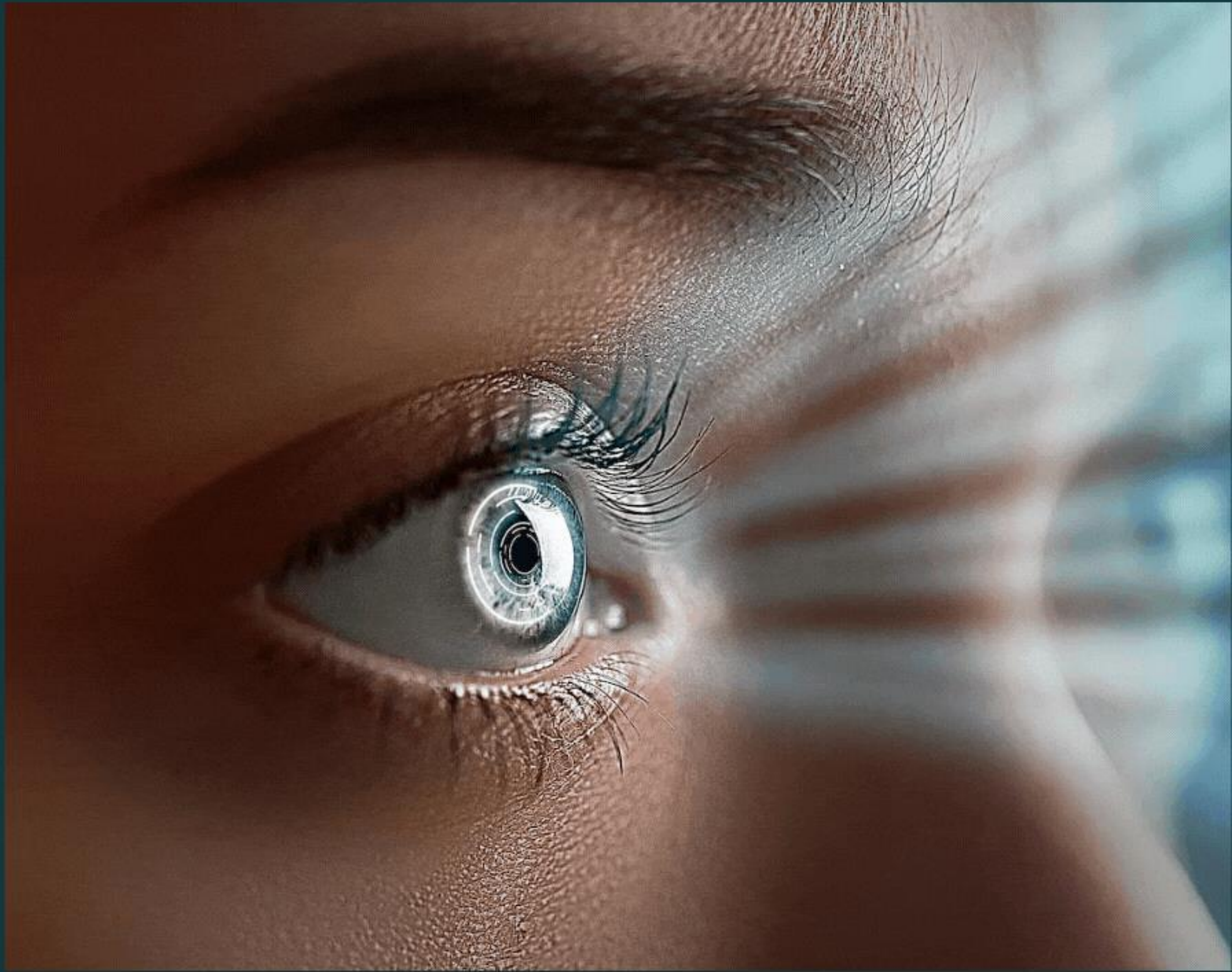




±

- To advise new solution of identification on the behavioral biometric to secure the access to the services
- Since deep method does not give excellent results, by using GAN solutions, it would allow to make data augmentation and thus improve the results of the deep method.

Thank you



Read the paper

Appendix

Classifiers parameters

❑ Classical machine learning models parameters

Table IV: Models parameters for the classical approach

Model	Parameters	Regression loss / Activate	Optimization Parameters	Maximal number of iterations	Regularization
Logistic Regression	–	–	–	–	Ridge (L2)
SVM	Cost : 1	ε : 0.1	Kernel : RBF	–	–
kNN	N^o of neighbors : 5	Metric : Euclidean	Weight : Uniform	–	–
AdaBoost	N^o of estimators : 50	Learning rate : 1.0	Regression loss function : Linear	–	–
Random Forest	N^o of trees : 10	–	–	–	–
Neural Networks	Neurons in hidden layers : 200	ReLU	solver : Adam	Max_{iter} : 500	α : 0.0001

❑ Deep learning models – Architecture's & Optimization's

Table V: Architecture's hyperparameters for the deep learning approaches

Methods	#Layers	#Conv	#Invar	Normalize	Pooling	Feature	Activate	Regularize
FCN	5	3	4	Batch	None	GAP	ReLU	None
ResNet	11	9	10	Batch	None	GAP	ReLU	Dropout

Table VI: Optimization's hyperparameters for the deep learning approaches

Methods	Algorithm	Valid	Loss	Epochs	Batch	Learning rate
FCN	Adam	$Split_{70\%}$	Entropy	250	10	0.001
ResNet	Adam	$Split_{70\%}$	Entropy	250	10	0.001