How Artificial Intelligence can be used for Behavioral Identification?

Yris Brice Wandji Piugie, Joël Di Manno, Christophe Rosenberger, Christophe Charrier

How Artificial Intelligence can be used for Behavioral Identification?

Yris Brice Wandji Piugie*†, Joël Di Manno*, Christophe Rosenberger† and Christophe Charrier†
*FIME EMEA, 14000 Caen, France
brice.wandji@fime.com, joel.dimanno@fime.com
†Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, 14000 Caen, France
christophe.rosenberger@ensicaen.fr, christophe.charrier@unicaen.fr

***Abstract*—Nowadays, users interact with computer systems. Behavioral biometrics consists of analyzing user's interactions for identification and verification applications. This approach could be very useful for enhancing security and improving user experience and many privacy concerns are also related. In this paper, we address the problem of user identification considering their behaviors. How efficient are classical machine learning methods on such data? What about deep learning approaches? We illustrate this work on two behavioral modalities namely human activity using smartphones and keystroke dynamics on a laptop. Since the accuracy rates of most behavioral biometrics modalities are lower than morphological ones, we consider two approaches for these modalities that can be represented as time series: classical machine learning and deep learning techniques. We intend to show that many algorithms can obtain very good performance for different modalities without any specific tuning to the considered modality. This comparative analysis allows us to show that behavioral biometrics can be used for security applications (i.e. who is accessing the company information system) but could be a privacy concern as a user could be identified while navigating on the Internet.**

***Keywords*-Behavioral biometrics; identification; privacy; machine learning; deep learning; keystroke dynamics**

I. Introduction

The development of information and communication technologies (ICT), as well as improvements in ambient intelligent technologies, such as sensors and smart phones, have led to the rapid development of smart environments [1], [2]. An enormous amount of resources can be saved if sensors can help staff record and monitor patients or automatically report any abnormal behavior [3], [4] like depicted in Figure 1.

In order to ensure the application of strong customer authentication, it is necessary to require adequate security features for the elements of strong customer authentication [1] categorised as 'knowledge' (something only the user knows), such as length or complexity, for the elements categorised as 'possession' (something only the user possesses), such as algorithm specifications, key length and information entropy, and for the devices and software that read elements categorised as 'inherence' (something the user is) such as algorithm specifications, biometrics sensor and template protection features,

[1]http://data.europa.eu/eli/reg_del/2018/389/oj

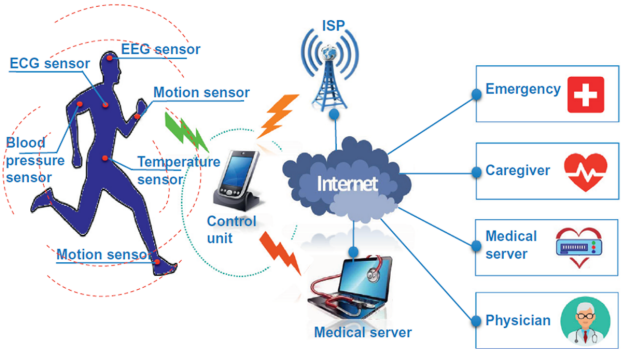


Figure 1: Framework for intelligent health care monitoring systems (HCMS) [5].

in particular to mitigate the risk that those elements are uncovered, disclosed to and used by unauthorised parties.

If Authentication is the ability to prove that a user is genuinely who that person claims to be, Identification is the ability to identify uniquely a user in a system. Within these contexts, behavioral biometrics permits to enhance user experience as user authentication/identification can be transparent for him/her (background processing).

This led us to ask the question how easy it is possible to identify a person based on his/her behavior such as with the keystroke dynamics even when users enter the same password? Can we recognize a person by the activities he or she has carried out? Identification is a multi-class classification problem. From the data, a chosen classifier distinguishes and identifies the user who has generated a given characteristics and feature sample, by returning the user ID (identification number or class) of the user to whom these characteristics belong [6]. However, biometric identification has an advantage over passwords as it is based on features that are specific to an individual and are not easy to duplicate or steal [7]. Another advantage for security (and maybe a drawback for privacy) is the possibility to use behavioral biometrics for transparent authentication solutions [8] where user' behaviors are constantly analyzed.

There are two main biometrics modalities namely morphological and behavior. Figure 2 gives examples for each biometric

modality. Behavioral biometric identification is the process of measuring a user's behavioural tendencies resulting from both psychological and physiological differences between individuals. It has been resumed by Bailey et al. that behavioral methods include keystroke dynamics, mouse dynamics, voice recognition, signature verification, and Graphical User Interface (GUI) usage analysis [6]. Due to the variability of the human body and mind, the adoption of this type of biometrics has lagged behind physiological biometrics [6]. Note that analyzing user activities and keystrokes dynamics does not require any extra hardware.

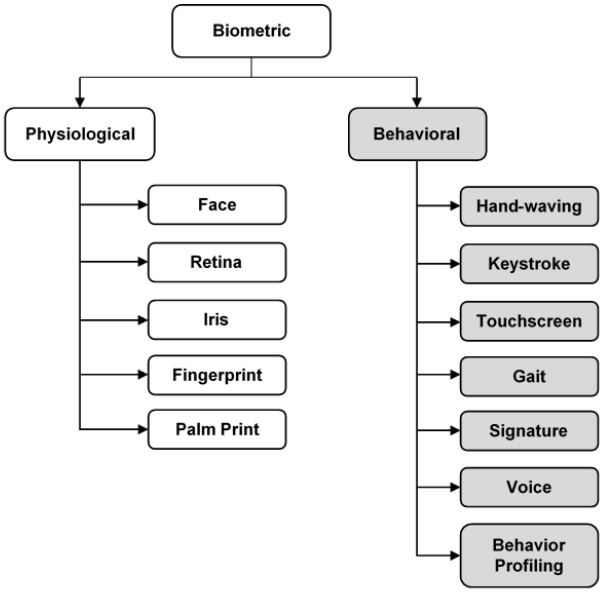


Figure 2: Biometrics modalities.

The performance of behavioral biometrics identification is lower than those of more traditional identification methods (related to morphological modalities) [6]. In this paper, we intend to answer how well a baseline machine learning approach could perform for user identification from behavioral biometrics data. We compare in this work different machine learning algorithms including deep learning for user identification based on its behavior described by time series. This paper highlights also the Orange data mining software and presents a very effective and simplistic way to perform data analysis work through machine learning classifiers. We consider two behavioral biometrics modalities namely physical activities (*laying*, *sitting*, *standing*, *walking*, *walking downstairs*, *walking upstairs*) acquired from a smartphone and keystroke dynamics on a laptop.

The paper is organized as follows. Section II contains related work on identification from user activities and keystroke dynamics systems. Section III presents the proposed method and the different machine learning models with the specifications and the impact of different parameters on our evaluation system. Section IV draws the experimental protocol. Section V details the experiments on benchmark datasets and the results we obtained. Section VI draws conclusions from our work.

II. Related work

In this section, we introduce the general characteristics of solutions proposed by researchers in this field for behavioral analysis for user identification.

A. Human activity

User identification has wide applications (logical access control, supervision...). The recent advancements of Artificial Intelligence (AI) have make the human being more inclined towards novel research aims in recognizing objects, learning the environment, time series analysis and predicting the forthcoming sequences [3]. Nowadays, there is a growing interest of AI researchers towards machine and deep learning which compromise massive applications in the field of speech recognition, language modeling, video processing and also time series analysis. Human Activity Recognition (HAR) is one of the challenging problems which seeks answers in this wonderful AI field. It can be mainly used for eldercare and childcare as an assisting technology combined with technologies like Internet of Things (IoT). Table I summarizes the assumptions required for the different algorithms described below.

Table I compares different classification techniques, different activities, different sources of input and finally the best performance that was obtained using a particular classifier.

B. Keystroke dynamics

Keystroke typing dynamics allows to profile users (identification, authentication, gender recognition, profiling) by analyzing the way a user is typing on a keyboard as for example when surfing on the Internet. Keystroke dynamics was first used in 1975 [15] and the basic idea was to use a keyboard to automatically identify individuals. In the preliminary report dressed by Gaines et al. [16], seven secretaries typed several paragraphs of text and the researchers showed that it was possible to differentiate users by their typing habits [17].
Keystroke dynamics is a two factor authentication scheme as we combine the knowledge of a password and the way of typing. In case of attack, it can be revoked by changing the password. Nevertheless, many studies showed it is possible to profile users on Internet (gender recognition, age category) [18] without the consent or awareness of the users [17]. Table II gives an overview of keystroke dynamics relative works.
These two behavioral biometrics modalities have been studied in the literature but not in a constrained context (i.e., we consider that we know what a person types on the keyboard, or that we know his activity) and a realistic context (i.e., we consider that we do not know what a person types on the keyboard, or that we do not know his activity). We would like to know in this work how efficient can be a generic machine learning approach for user identification in such contexts.

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%

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

III. Proposed method

In this work, we consider behavioral biometric data represented as times series. We want to assess the capability of machine learning methods to obtain good performance on user identification. We use two main approaches. The first approach consists of using classical classifiers by using raw data as input. We consided the following machine learning classifiers: Support vector machine (SVM), Neural Networks (NN), Random Forest (RF), AdaBoost, Logistic Regression, Naive Bayes, k-Nearest Neighbor (k-NN) and Stacking (fusion of classifiers). Second, we inted to test deep learning techniques that consists in optimizing the representation of raw data to enhance user identification. We considered the following architectures: Fully Convolutional Neural Networkss (FCN) and Residual Network (ResNet) used in [25].

A. Classical machine learning approaches

For this work, we use the Orange data mining software. It is an open-source data visualization, machine learning and data mining toolkit [26]. It features a visual programming front-end for explorative data analysis and interactive data visualization, and can also be used as a Python library. The software is developed by University of Ljubljana under GNU General Public License since 1997.

We designed a data workflow composed of widgets (data processing unit) with Orange as depicted by Figure 3. This workflow can be used for any behavioral biometrics data and generates performance metrics. Import and preprocessing database sub-workflow is illustrated in *Block 1*. *Block 2* represents seven widgets associated to the following 7 classifiers: SVM, NN, RF, AdaBoost, Logistic Regression, Naive Bayes and k-NN [5], [26]. Using the stacking widget in *Block 3* permits to fusion the different classifiers. In order to evaluate the performance of the defined workflow, it is preprocessed by the Test and Score widget. We use *Block 4* for the evaluation of this system by computing the confusion matrix and ROC curve. *Block 5* allows a visual inspection of the obtained predictions.

B. Deep learning approaches

After having presented an overview of the generic workflow on the Machine Learning approach as well as the models carried with Orange, we used FCN and ResNet as Deep Learning architectures all described in [25] for time series classification that we compare in this article.

IV. Experimental protocol

In this section, we present the experimental protocol we follow in this work.

A. Behavioral datasets

The UCI-HAR dataset used for the activity modality is the standard Human Activity Recognition (*HAR*) dataset which

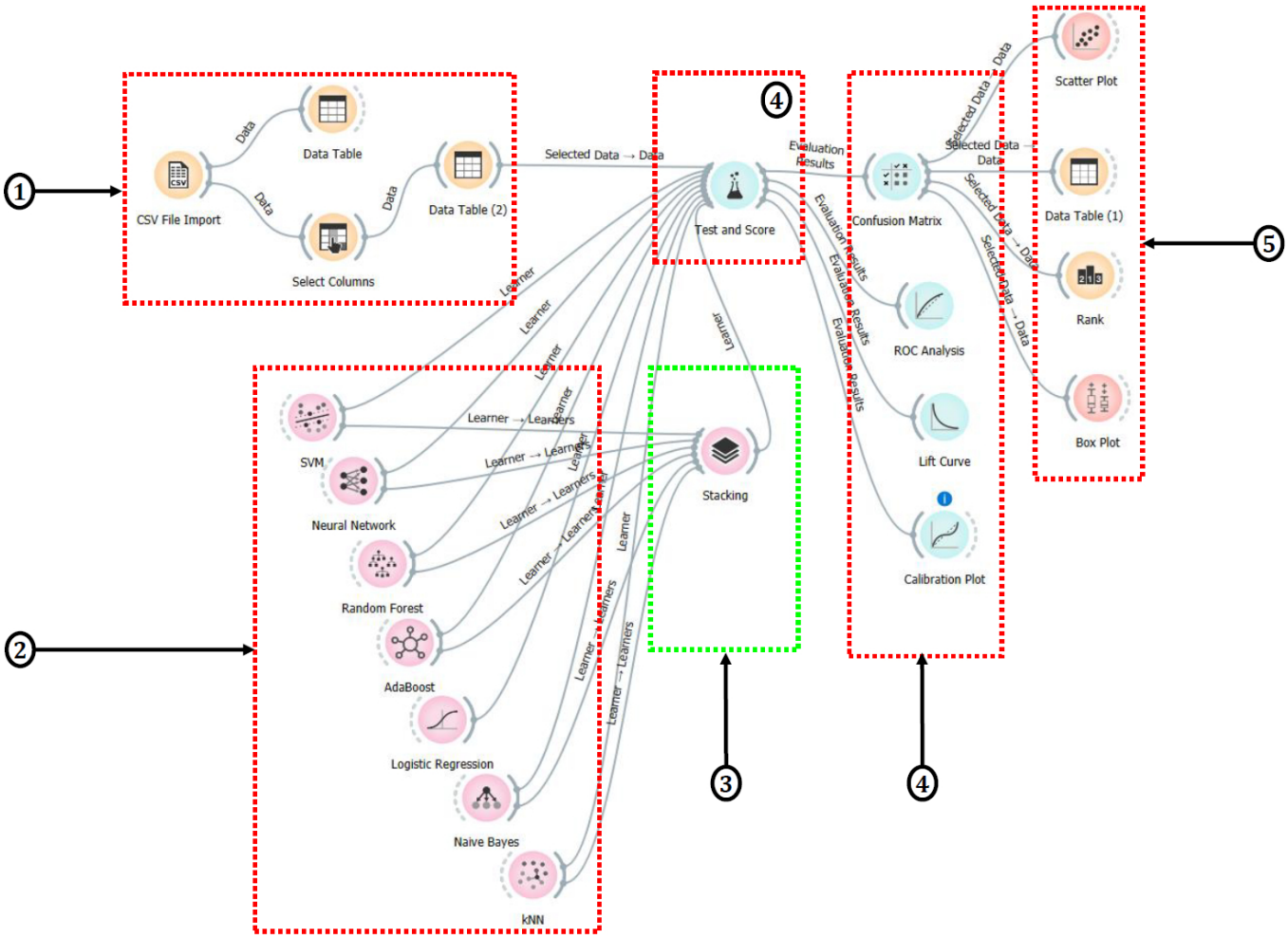


Figure 3: Global workflow for user identification from behavioral data.

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

was made available in 2012 [14]. This is available and can be downloaded from the *UCI* machine learning repository. Size of the dataset is 10299 samples. The data has been collected using 30 persons aged between 19 and 48 performing six standard activities namely *walking*, *walking upstairs*, *walking downstairs*, *sitting*, *standing* and *laying*. Each person has performed this sequence of activities twice once with the device on their left-hand side and once with the device on their right-hand side. Sensors used were count sensor (accelerometer) and the position waist sensor (gyroscope). Data has been collected with *Samsung Galaxy S II* mobile phone. Here they have captured accelerometer and gyroscope 3-axial raw signals with *tAcc-XYZ* and *tGyro-XYZ* with 50Hz frequency. The experiments have been video-recorded to label the data manually. The obtained dataset has been randomly partitioned into two sets, where 70% of the volunteers was selected for generating the training data and 30% the test data.

The GREYC-NILSLAB dataset [27] for keystroke dynamics is constituted of 5 passwords entered by 110 users. The best password is a sentence according to experts [28]. For keystroke dynamics modalities, 5 passphrases were presented to users as shown in Table III, which are between 17 and 24 characters (including spaces) long, chosen from some of the well-known or popular names or artists (known both in France and Norway), denoted P1 to P5. All of the participants were asked to type these 5 different passphrases 20 times. The

GREYC Keystroke software [29] has been used to capture biometric data.
Keystroke dynamics is a viable and convenient way to supplement security for identity verification [29].

B. Performance analysis

The performance evaluation metrics used in this work are Classification Accuracy (CA), Precision (P), recall (R), Area Under Curve (AUC) and Cumulative Match Characteristic (CMC). T_P, T_N, F_P and F_N represent true positives, true negatives, false positives and false negatives respectively. There are the following definitions:

1) Classification Accuracy (CA): For a given test dataset, the ratio of the number of samples correctly classified to the right user by the classifier compared to the total number of samples. This metric (also called rank1 accuracy) formula is given by the following equation

$$A = \frac{T_P + T_N}{T_P + T_N + F_P + F_N} \tag{1}$$

2) Precision (P): The ratio of the number of correctly identified positive samples (corresponding to the right individual) to the total number of samples identified as positive in the identified sample. The computation formula is given by the following equation:

$$P = \frac{T_P}{T_P + F_P} \tag{2}$$

The precision score can be the number of correct predictions made divided by the total number of predictions made.

3) Recall (R): The recall rate is the ratio of the number of positively identified individuals correctly identified to the total number of positive samples in the total sample used. The recall rate is how many positive samples are identified. The calculation formula is:

$$R = \frac{T_P}{T_P + F_N} \tag{3}$$

4) Area Under the Curve (AUC): It computes the area under the curve when plotting the precision versus the recall value. It should be as high as possible (maximal value is 100% or 1).
5) Cumulative Match Characteristic (CMC) Curve: It is a method of showing the measured accuracy performance of a biometric system operating within an identification task. Templates are compared and ranked based on their similarity. The CMC indicate how often the biometric subject template appears in the ranks (1, 5, 10, 100, etc.) based on the match rate. A CMC compares the rank (1, 5, 10, 100 etc.) versus identification rate.

C. Classifiers parameters

In this subsection, we list the different parameters used through the learning methods. Table IV gives model parameters defined in Orange for the classic basic approach. Tables V and VI show respectively the architecture and the optimization hyperparameters for the deep learning approaches. A model checkpoint procedure was performed either on the training set or a validation set (split from the training set). Which means that if the model is trained for 250 epochs, the best one on the validation set (or the train set) loss will be chosen for evaluation. This characteristic is included in Table VI under the *valid* column. In addition to the model checkpoint procedure), models in Table V were initialized randomly using Glorot [30] which is a uniform initialization method. Models were optimized using a variant of Stochastic Gradient Descent (SGD) such as Adam [31] and AdaDelta [32].

V. Results and Discussion

All experiments in this research work were conducted in the same environment which is composed of: Windows 10 Pro operating system, Intel(R) Core (TM) CPU @ 1.8GHz, 8GB RAM, and TensorFlow 2.2.0 - G.P.U. on Python 3.8.2. Then, the system was tested using the following datasets:

1) UCI-HAR database,
2) GREYC-NISLAB database.

A. Classical machine learning

The used models in the classical approach and developed in our system are evaluated in terms of AUC, CA, P and R. Table VII gives classification result from UCI-HAR database. Table VIII gives classification results from GREYC-NISLAB database. We can see in these two tables that the fusion of classifiers (Stack) provides very good results on both datasets. After merging the five passwords, Table IX gives the results of classification accuracy when identifying a person with knowledge of how they type on a keyboard.
We can therefore identify a person knowing his typing style, the type of hand used, his gender, and his age with a clearly classification accuracy of 98.18%, 99.27% 88.73% and 70.73% respectively.

B. Deep learning techniques

The used models for deep learning approach are evaluated in terms of CA, P and R. The performance metrics for both modalities are provided in Tables X. We see that from our two behavorals modalilities, ResNet deep classifier perform better than FCN on user identification. The Obtained results are worst than classical machine learning (the datasets are probably not enough large to obtain better results).

C. Discussion

This paper presents a study on how it is easy to define a user identification method given behavioral biometrics data.
The UCI behavior recognition dataset is collected by measuring the six daily behaviors of the 30 participants. The experiment uses a three-axis embedded accelerometer and a gyroscope operating at 50 Hz. The three component values of the accelerometer and the gyroscope are obtained separately, and the data dimension is 561.
Obtained results in Table VII for user identification through his/her activity shows us that stacking model performs well

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

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	$\text{Split}_{70\%}$	Entropy	250	10	0.001
ResNet	Adam	$\text{Split}_{70\%}$	Entropy	250	10	0.001

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

with a precision score of 93.90% than the seven other models in Orange workflow. Like depicted in Table VIII, we have the best precision with the staking model and this with all the keystroke P1 (63.67%), P2 (72.15%), P3 (66.10%), P4 (79.64%) and P5 (84.30%) databases. With a fusion of features (P_T), we obtain 98.30% score of precision. This means that the larger our behavioral database, the higher the classification score. So far considering these model comparisons on different behavioral biometrics databases, it comes out that the stacking model performs well. This shows that methods evaluated in this work highly successful identity user from behavioral biometrics data.

Another study that used deep Neural Networks notably ResNet and FCN achieved a precision rate of 87.20%, 80.09% respectively for HAR dataset and 82.94%, 78.95% for the fusion of dynamic keystrokes feature P_T dataset. In view of these comparisons, we say that ResNet performs more than FCN for both behavioral modalities in detecting the user than the other models described in [25].

We tested in this work complicated databases because the idea was to recognize a person just from his/her behavior. However, in the literature, there is little work on the identification of individuals using the dynamics keystroke with low classification accuracy.

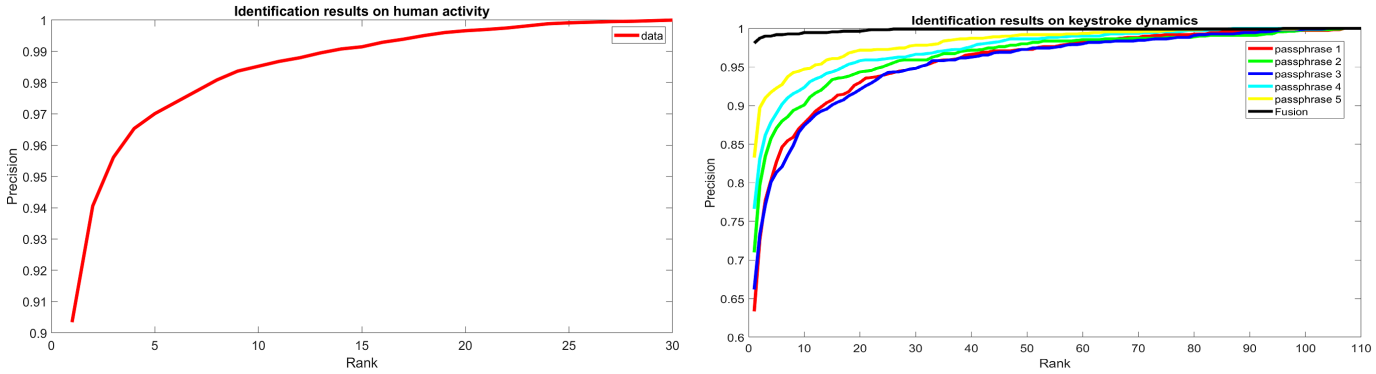
We compute the rank 3 identification accuracy in order to know how many times the individual has been identified with the 3 most likely. The obtained results conducted on the two datasets show that the classification rate obtained by the best machine learning model (Stacking) is 93.90% for human activity and 98.10% for fusion of the keystroke dynamics features. Using the cumulative matching characteristic (CMC) curve, we show that for our best model (Stacking), an individual appears in rank 3 (the three most likely) for a match rate of 95.61% for human identity recognition and a matching rate of 99.00% for the fusion of keystroke dynamics identification.

Interpreted by Table XI, Figure 4 is used to compare the performance of the biometric identification system. The depicted curves represent the values of the identification rank and the probabilities of a correct identification less than or equal to these values, respectively on x-axis and y-axis.

Figure 4a allows us to observe that the probability of identifying one person is 90.34%, the probability of identifying 2 persons is 94.06% and the probability of identifying 3 persons is 95.61% in the UCI-HAR database. Figure 4b is interpreted by Table XI. The database fusionned P_T gives 99.00% as rank 3 score. The fourth column of the Table XI gives the rank 3

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



((a)) CMC HAR

((b)) CMC curve Keystroke Dynamics

Figure 4: CMC curve of Stacking model in Orange workflow

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

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

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

for each keystroke P1 to P5.

Ensuring strong security for Identification and keeping privacy is key when developing and deploying any new technology. This paper shows that Machine Learning solution, specifically Stacking, can be a reliable help for Identification and can be used through Multi Identification Factors solutions to reach very high level of confidence. Identification with two factors might be appropriate in some circumstances, but too much in others. Behavioral with Machine Learning and Deep Learning enables multimodality authentication without increasing the burden on the user. Moreover, it is essential to build confidence and trust, especially for technologies which processes our personal data. Machine Learning and Deep Learning using

Table XI: HAR and keystroke rank scoring

Dataset	rank1 (%)	rank2 (%)	rank3 (%)
HAR	**90.34**	**94.06**	**95.61**
PT	**98.09**	**98.73**	**99.00**
P1	63.36	72.64	77.73
P2	71.00	79.73	83.45
P3	66.18	73.27	77.18
P4	76.64	83.09	86.18
P5	83.27	89.73	91.00

behavioral for Identification can be a key of success but also a way to classify individuals into Targets or Groups, without consent of the users.

VI. Conclusion

In this paper, we present a baseline approach for user identification based on multimodal behavioral biometrics using machine learning (classical and deep learning). Two behavioral biometrics have been studied: human activities captured by a smartphone and Keystroke dynamics on a laptop. We proposed a generic workflow for the classical approach (machine learning) using Orange data mining software. We used the most recent successful deep learning approaches for time series classification since the identification is the result of a classification problem.

In the classical approach, users are classified by using eight different machine learning methods namely Support Vector Machine (SVM), Neural Networks (NN), Random Forest, AdaBoost, Logistic Regression, Naive Bayes, k-Nearest Neighbor (k-NN) and stacking in Orange data mining software for both modalities. With Deep Learning approach, we compared result

from time series classification by comparing these models, Fully Convolutional Neural Networks (FCN) and Residual Network (ResNet) by using TensorFlow 2.2.0 - G.P.U. on Python 3.8.2.

Our results show that end-to-end deep learning can achieve the current state-of-the-art performance for time series classification with architectures such as FCN and deep ResNet.

This comparative analysis allows us to show that behavioral biometrics can be used for security applications (i.e. who is accessing the company information system) but could be a privacy concern as a user could be identified while navigating on the Internet. These frictionless solutions are great opportunities for improving user experience but could be a threat for our data privacy as our behavior could permit to classify some of our traits without control. We will use these behavioral biometrics modalities in the area of authentication in the future coming paper.

ACKNOWLEDGMENT

Authors would like to thank FIME EMEA, the "Normandy Region" and the ANRT for their financial support of this work.

REFERENCES

[1] M. D. Lytras, A. Visvizi, L. Daniela, A. Sarirete, and P. Ordonez De Pablos, "Social networks research for sustainable smart education," *Sustainability*, vol. 10, no. 9, p. 2974, 2018.

[2] A. Visvizi, J. Jussila, M. D. Lytras, and M. Ijäs, "Tweeting and mining oecd-related microcontent in the post-truth era: a cloud-based app," *Computers in Human Behavior*, vol. 107, p. 105958, 2020.

[3] A. Rasekh, C.-A. Chen, and Y. Lu, "Human activity recognition using smartphone," *arXiv preprint arXiv:1401.8212*, 2014.

[4] Y. B. W. Piugie, D. Tchiotsop, A. N. K. Telem, and E. B. M. Ngouonkadi, "Denoising of electroencephalographic signals by canonical correlation analysis and by second-order blind source separation," in *2019 IEEE AFRICON*. IEEE, 2019, pp. 1–8.

[5] A. Subasi, K. Khateeb, T. Brahimi, and A. Sarirete, "Human activity recognition using machine learning methods in a smart healthcare environment," in *Innovation in Health Informatics*. Elsevier, 2020, pp. 123–144.

[6] K. O. Bailey, J. S. Okolica, and G. L. Peterson, "User identification and authentication using multi-modal behavioral biometrics," *Computers & Security*, vol. 43, pp. 77–89, 2014.

[7] C. Rosenberger, "Les identités numériques et l'authentification," 2020.

[8] Y. Ashibani and Q. H. Mahmoud, "A multi-feature user authentication model based on mobile app interactions," *IEEE Access*, vol. 8, pp. 96 322–96 339, 2020.

[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.

[15] R. Spillane, "Keyboard apparatus for personal identification," *IBM Technical Disclosure Bulletin*, vol. 17, p. 3346, 1975.

[16] R. S. Gaines, W. Lisowski, S. J. Press, and N. Shapiro, "Authentication by keystroke timing: Some preliminary results," Rand Corp Santa Monica CA, Tech. Rep., 1980.

[17] D. Migdal and C. Rosenberger, "Statistical modeling of keystroke dynamics samples for the generation of synthetic datasets," *Future Generation Computer Systems*, vol. 100, pp. 907–920, 2019.

[18] S. Z. S. Idrus, E. Cherrier, C. Rosenberger, and P. Bours, "Soft biometrics for keystroke dynamics: Profiling individuals while typing passwords," *Computers & Security*, vol. 45, pp. 147–155, 2014.

[19] S. P. Banerjee and D. L. Woodard, "Biometric authentication and identification using keystroke dynamics: A survey," *Journal of Pattern Recognition Research*, vol. 7, no. 1, pp. 116–139, 2012.

[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.

[25] H. I. Fawaz, G. Forestier, J. Weber, L. Idoumghar, and P.-A. Muller, "Deep learning for time series classification: a review," *Data Mining and Knowledge Discovery*, vol. 33, no. 4, pp. 917–963, 2019.

[26] J. Demšar, T. Curk, A. Erjavec, Črt Gorup, T. Hočevar, M. Milutinovič, M. Možina, M. Polajnar, M. Toplak, A. Starič, M. Štajdohar, L. Umek, L. Žagar, J. Žbontar, M. Žitnik, and B. Zupan, "Orange: Data mining toolbox in python," *Journal of Machine Learning Research*, vol. 14, pp. 2349–2353, 2013. [Online]. Available: http://jmlr.org/papers/v14/demsar13a.html

[27] S. Z. Syed Idrus, E. Cherrier, C. Rosenberger, and P. Bours, "Soft biometrics database: A benchmark for keystroke dynamics biometric systems," in *2013 International Conference of the BIOSIG Special Interest Group (BIOSIG)*, 2013, pp. 1–8.

[28] S. Z. S. Idrus, E. Cherrier, C. Rosenberger, and P. Bours, "Soft biometrics for keystroke dynamics," in *International Conference Image Analysis and Recognition*. Springer, 2013, pp. 11–18.

[29] R. Giot, M. El-Abed, and C. Rosenberger, "Greyc keystroke: a benchmark for keystroke dynamics biometric systems," in *2009 IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems*. IEEE, 2009, pp. 1–6.

[30] X. Glorot and Y. Bengio, "Understanding the difficulty of training deep feedforward neural networks," in *Proceedings of the thirteenth international conference on artificial intelligence and statistics*. JMLR Workshop and Conference Proceedings, 2010, pp. 249–256.

[31] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," *arXiv preprint arXiv:1412.6980*, 2014.

[32] M. D. Zeiler, "Adadelta: an adaptive learning rate method," *arXiv preprint arXiv:1212.5701*, 2012.