Behavioral Biometric Authentication on Mobile Devices

Wael Elloumi (R&D Worldline)
Aladine Chetouani (Prisme Laboratory)

Worldline

Agenda

1. Introduction
2. BioTyping authentication
3. Continuous behavioral biometric authentication
4. Conclusion

Introduction

Biometrics in a nutshell

Definition

The automatic identification or verification of living individuals by using their physiological and behavioral characteristics

Classification

Physiologic
Digital fingerprint, Iris, Face
Vein, DNA

Behavior
Voice, gait, keystroke dynamics…

Issues to consider

- **Identification** or **verification**?
- **Data protection**
- **Presentation attacks aka ‘spoofing’**
- **Life cycle** : Process of Enrollment – Verification – Repudiation - Fallback
- **Matching on user device** vs on server
- **Evaluation & certification**

BioTyping Authentication

PRISME

Laboratoire Pluridisciplinaire de Recherche Ingénierie des Systèmes, Mécanique, Énergétique

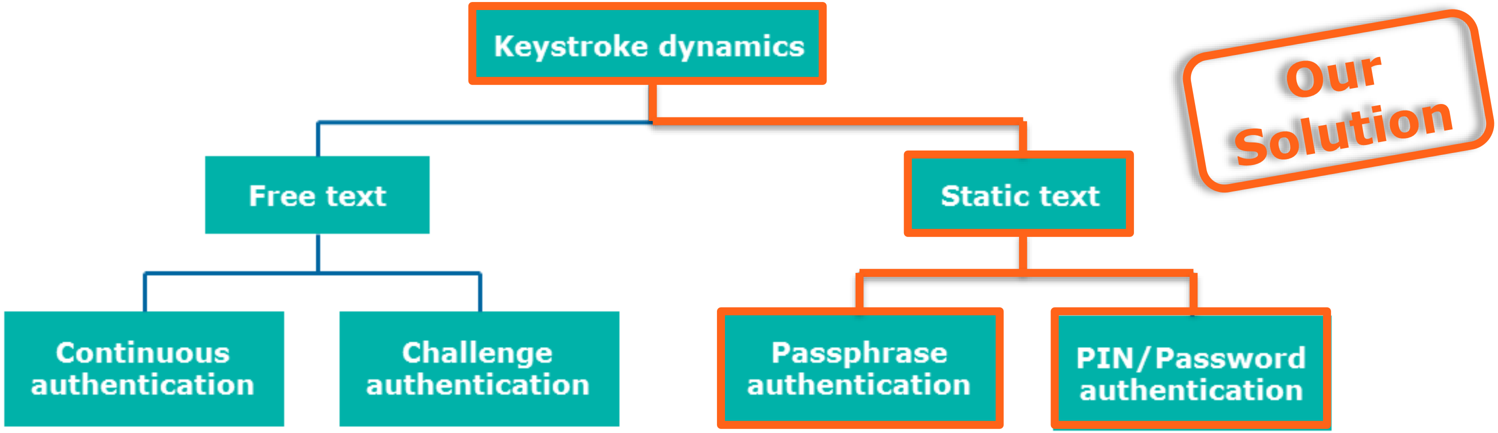
Worldline

BioTyping overview

Definition

Keystroke dynamics or BioTyping is **a behavioral biometric modality** used to **authenticate individuals** through their **way of typing** (patterns of rhythm, timing, etc.) on a keyboard

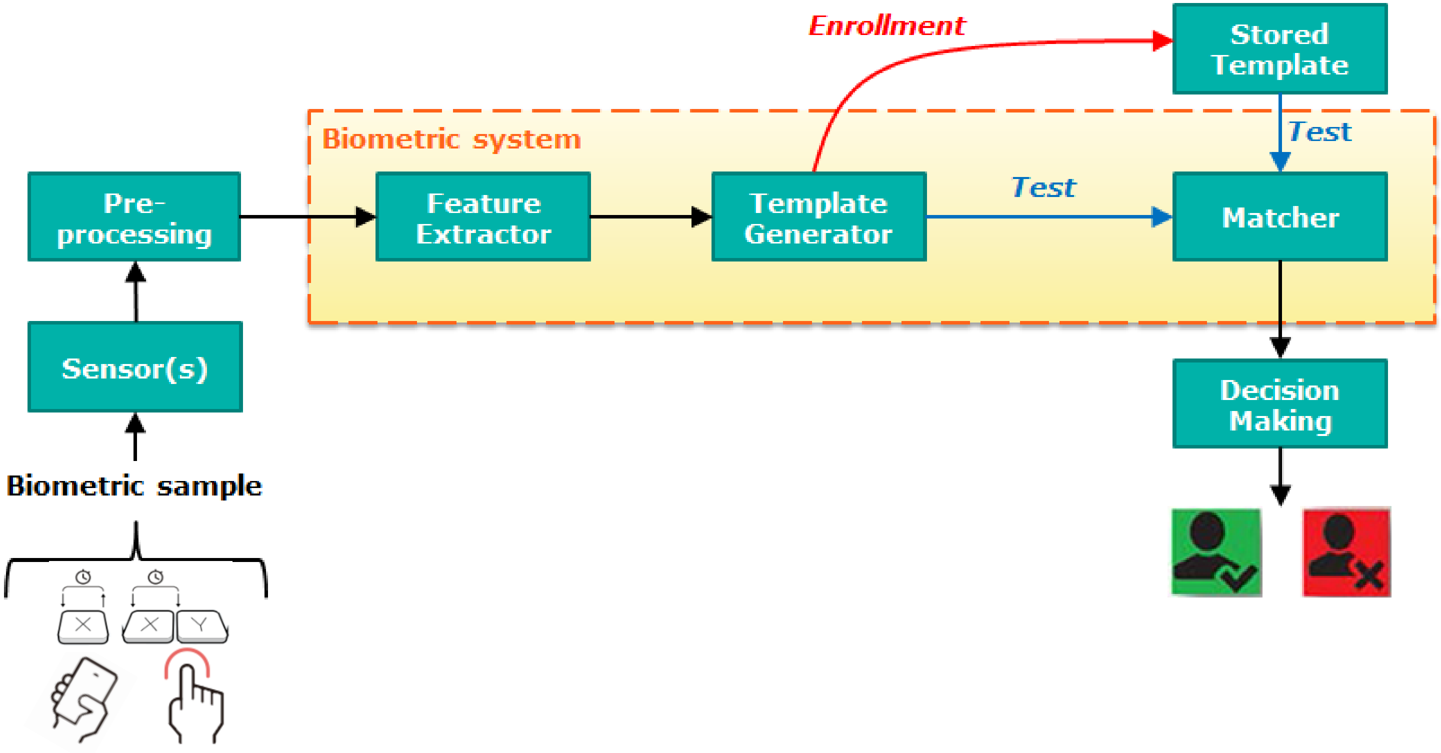
Taxonomy of keystroke dynamics systems



Purposes

- Enhance the security of PIN code based authentication on mobile devices
- Add an extra layer of security control based on BioTyping
- Monitor the way user enters his **PIN code**
  - **Transparent** enrollment
  - **Continuous** update of biometric template
  - **Seamless** authentication
- Maximum level of user control and **privacy**
  - **Record, storage and match on user device**
  - **No database, no server**

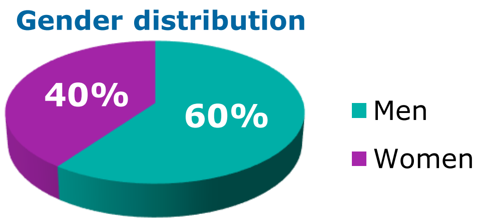
General framework

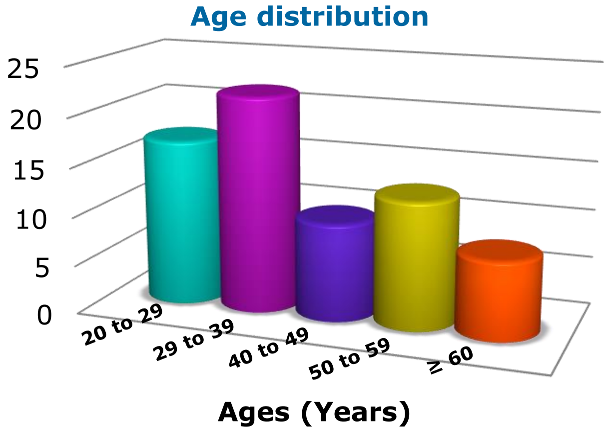


Methodology

Data collection

- **70 subjects** from Worldline were part of this study
- All participants were asked to enter the same six-digit PIN code (024680)
- The same acquisition device (**Nexus 5X**) for all subjects
- Data were collected **during 6 months** and over **4 sessions**
  - Each subject typed the PIN code **100 times (25 times per session)**
  - No more than two sessions per week were authorized
  - At least two days interval between two successive sessions
  - A brief practice session of 10 repetitions before each session acquisition

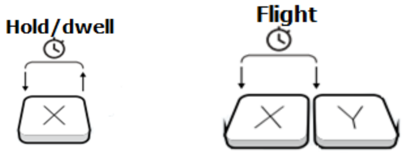




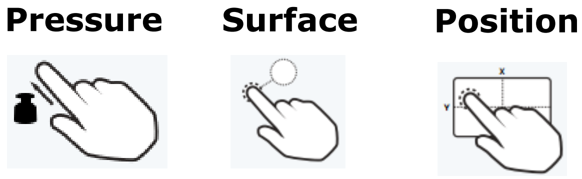
Methodology

Feature extraction

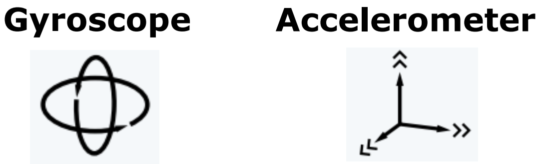
- **Timing features (22 features)**
  - Hold time or dwell time of individual keys
  - Key latencies or flight time between two consecutive keys
  - Overall typing speed (the global typing time)



- **Spatial feature (62 features)**
  - Touch pressure (TP)
  - Touch size (TS)
  - Touch position (Xpos, Ypos)



- **Motion features (456 features)**
  - Gyroscope
  - Accelerometer



In total 540 features are extracted for a 6-digit PIN code

Methodology

Evaluation methodology

1. Designate one of the 70 subjects as the genuine user and the rest as imposters
2. Split each imposter data into two equal parts for training and testing
3. Use 10-Fold Cross Validation to split genuine data into training data (90 samples) and testing data (10 samples)
4. Select 2 random samples from each imposter training data and 2 random samples from each imposter testing data
5. Train the model on the training data composed of 90 genuine samples and 138 imposter samples

Methodology

Evaluation methodology

6. Test the generated model on the testing data

7. Repeat the steps from 3 to 6 30 times and compute the average of EER, FRR and FAR for the designated genuine user

8. Repeat the whole process by designating each of the other subject as the genuine user in turn and compute the average of EER, FRR and FAR over all the users. Over a total of 21000 scores (70 subjects * 10 CV repetition * 30 random selection)

Experimental results

Classifier comparison

Classifier	Avg EER (%)	Avg FRR (%)	Avg FAR (%)	Avg ACC (%)
Random Forest	**1,15**	**0,45**	**0,84**	**99,52**
SVM	1,59	0,66	1,17	99,31
KNN	7,76	6,11	4,48	94
Naïve Bayes	11,04	7,66	8,17	92,31
Neural Network	4,53	4,82	0,37	95,48

Random Forest performs the best followed by the SVM classifier

Experimental results

Feature type comparison

	Random Forest			SVM		
Feature Type	**Avg EER (%)**	**Avg FRR (%)**	**Avg FAR (%)**	**Avg EER (%)**	**Avg FRR (%)**	**Avg FAR (%)**
Time (TM)	9,91	4,77	9,49	17,25	12,38	15,92
Spatial	5,05	1,2	4,33	5,20	3,94	2,60
Motion	1,89	0,96	1,18	2,47	1,57	1,34
Combined	**1,15**	**0,45**	**0,84**	**1,59**	**0,66**	**1,17**

Experimental results

Impact of the data normalization

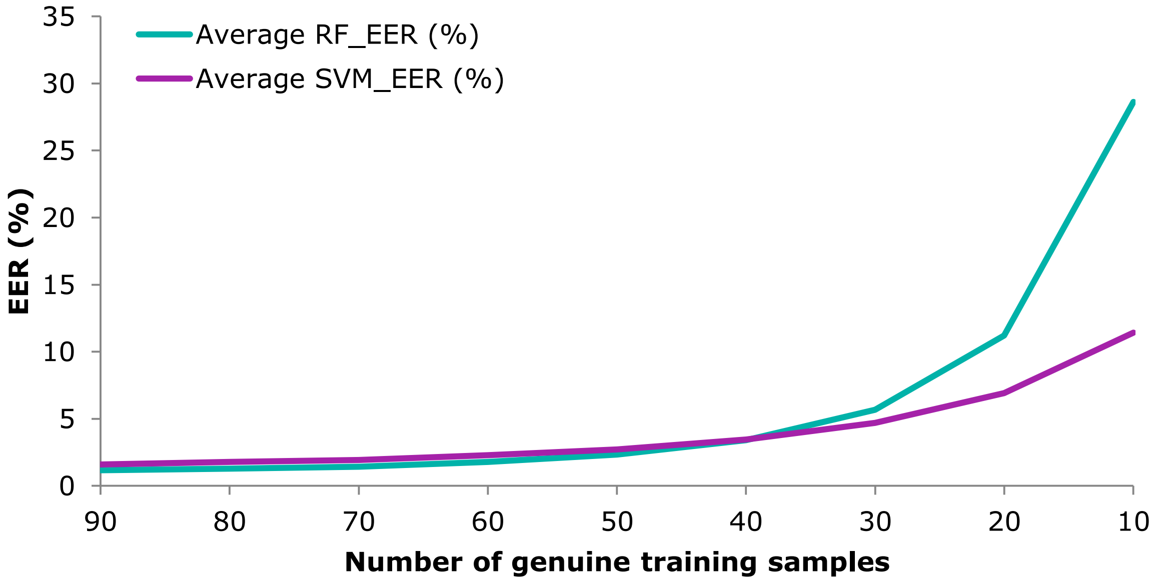
	Random Forest			SVM		
Normalization method	**Avg EER (%)**	**Avg FRR (%)**	**Avg FAR (%)**	**Avg EER (%)**	**Avg FRR (%)**	**Avg FAR (%)**
MinMax	1,16	0,46	0,85	1,58	0,65	1,15
ZScore	**1,14**	**0,45**	**0,82**	1,58	0,66	1,15
SD	1,15	0,44	0,85	**1,57**	**0,65**	**1,15**
Without	1,15	0,45	0,84	1,59	0,66	1,17

No significant impact of data normalization for both classifiers

Experimental results

Impact of the number of training samples

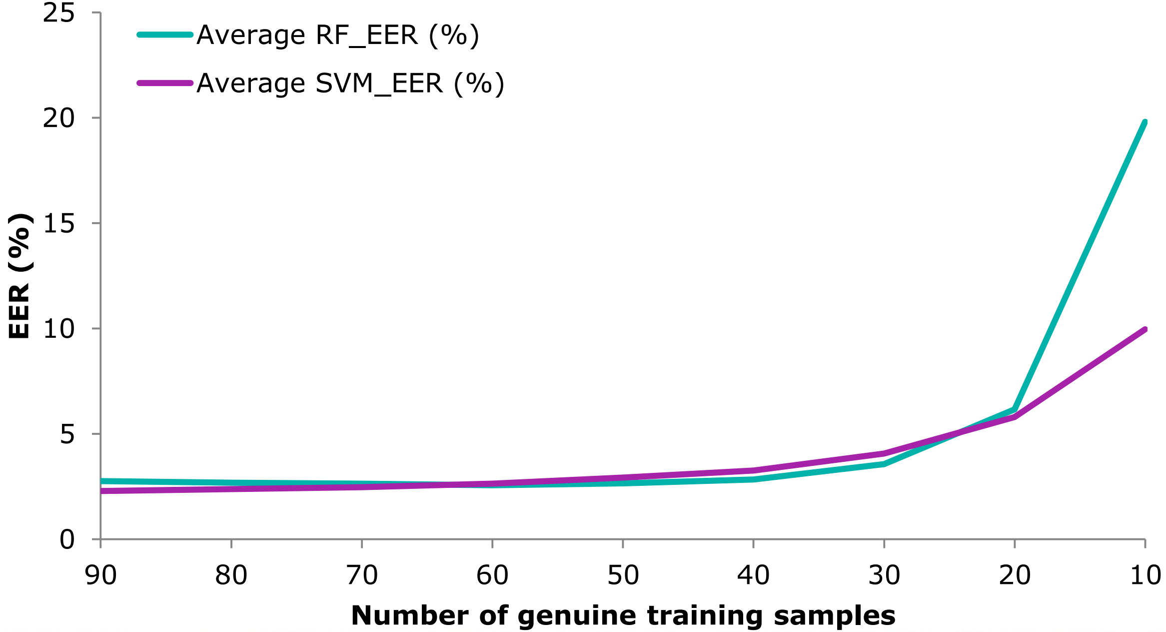
- Range of genuine samples: from 90 to 10 samples
- Number of imposter samples: 138 (2 random samples per imposter)



Experimental results

Impact of the number of training samples

- Range of genuine samples: from 90 to 10 samples
- Number of imposter samples: 69 (1 random sample per imposter)



Continuous Authentication

PRISME

Worldline

Purposes

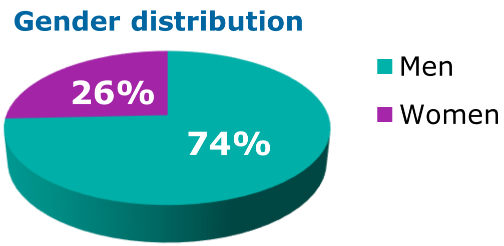
- Propose a risk-based and frictionless online payment authentication in the context of 3D secure 2.0
- Explore the continuous biometric authentication in addition to contextual data of the transaction
- Add an extra layer of security control based on behavioral biometrics
- Monitor the way user interacts with his smartphone when navigating on his mobile device browser, in-app or also in digital wallet
    - **Transparent** enrollment
    - **Continuous** update of biometric template
    - **Seamless and continuous** authentication
- Maximum level of user control and **privacy**
    - **Record, storage and match on user device**
    - **No database, no server**

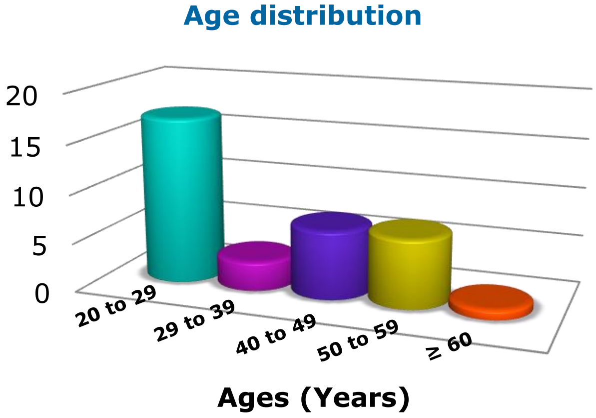
Worldline

Methodology

Data collection

- **35 subjects** from Worldline were part of this study
- All participants were asked to navigate on two predefined e-commerce websites in accordance to their own preference and habit
- The same acquisition device (**Nexus 5X**) for all subjects
- Data were collected **during 5 weeks** and over **4 sessions**
    - Using a chrome extension for touch features and an android service for motion features
    - Each experiment took roughly 10 minutes
    - At least two days interval between two successive sessions



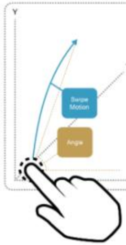


Methodology

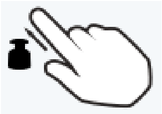
Feature extraction

- **Swipe (131 Features)**
  - Touch pressure, size, position and motion
  - Duration, velocity
  - Curve, direction, etc.
- **Tap (61 Features)**
  - Touch pressure, size and position
  - Duration, motion
  - Etc.
- **Motion features (20 Features)**
  - Gyroscope
  - Accelerometer
- **Zoom** (not widely used)

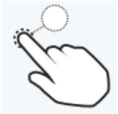
Motion



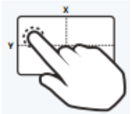
Pressure



Surface

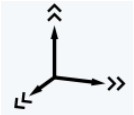


Position



Gyroscope

Accelerometer



Worldline

Methodology

Evaluation methodology

1. Designate one of the 35 subjects as the genuine user and the remaining users as imposters
2. Select randomly imposter's samples equal to the genuine samples to have a balanced data
3. Use 10-Fold Cross Validation to split genuine data into training data (90%) and testing data (10%)
4. Train the model on the training data composed of the genuine samples and imposters samples

Methodology

Evaluation methodology

5. Test the generated model on the testing data and calculate the average of Accuracy, EER, FRR and FAR

6. Repeat the steps from 2 to 5 for 4 times and compute the average of EER, FRR and FAR for the designated genuine user

7. Repeat the whole process by designating each of the 35 subjects as the genuine user in turn and compute the average of Accuracy, EER, FRR and FAR over all the users.

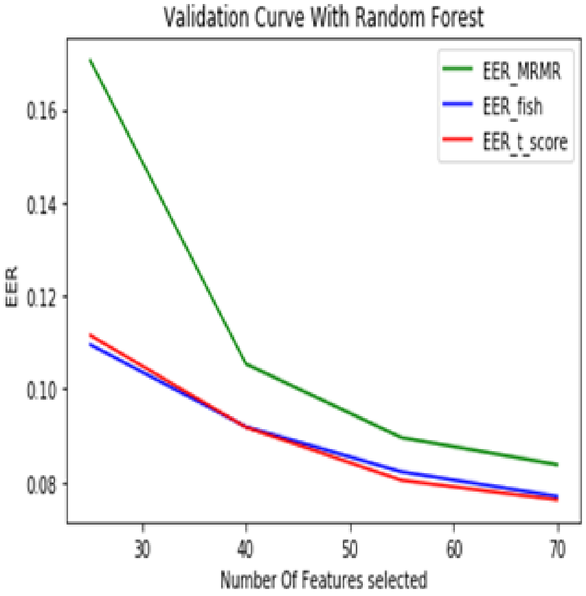
Experimental results

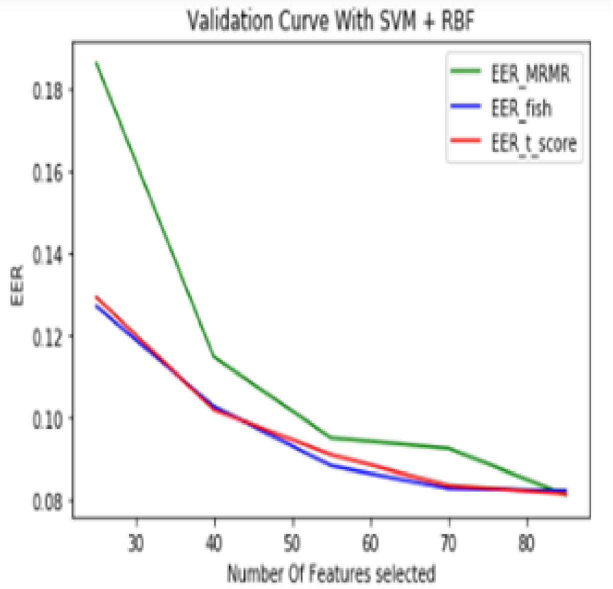
Classifier comparison

Classifier	Avg EER (%)	Avg FRR (%)	Avg FAR (%)	Avg ACC (%)
Random Forest	7,3	7	7,8	92,5
SVM	**6,7**	**6,5**	**7,6**	**92,9**

Experimental results

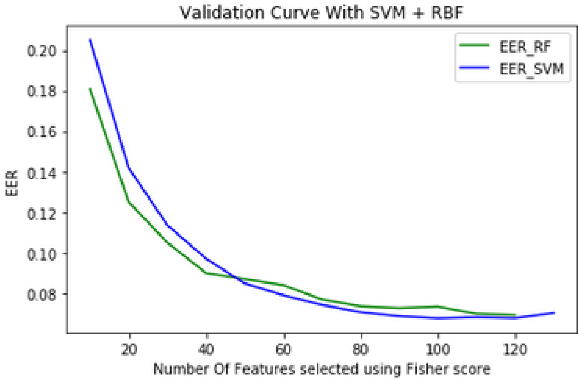
Feature Selection Methods

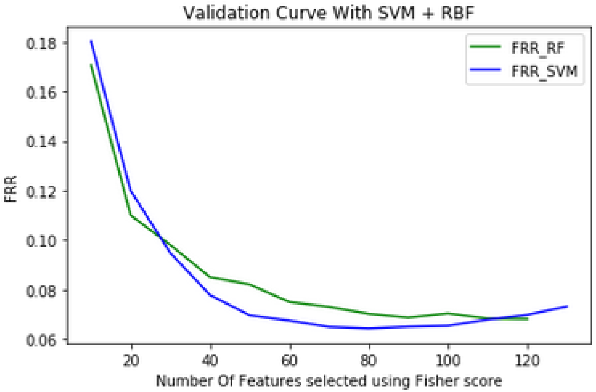


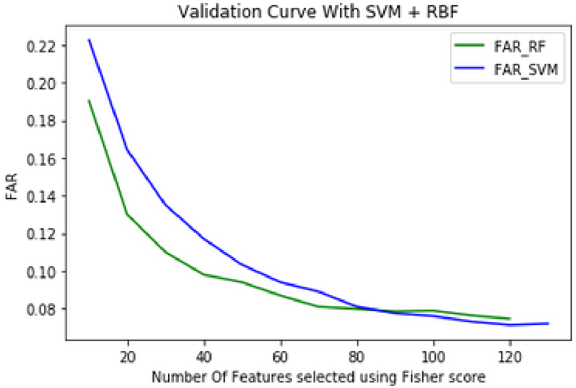


Experimental results

Feature Selection







Conclusion

Conclusion

To summarize

- **Behavioral biometrics authentication** is **increasingly needed** in various types of applications thanks to its convenience for:
  - **Security**
  - **User experience**
- Two studies are carried out on mobile behavioral biometric authentication
  - Approaches are validated on real databases
  - Obtained results are encouraging
- Work is still in progress
  - Design and development of PoCs
  - Feedback of our operational teams and clients

R&D

Thank you!