AGH

Continuous authentication on mobile devices using behavioral biometrics

Jakub Dybczak, Piotr Nawrocki

AGH University of Science and Technology

INFORMATYKA
Akademia Górniczo-Hutnicza w Krakowie

Motivation

Static (one-shot) authentication have some cons:

- does not offer security over a session,
- some methods are easy to be leaked (passwords, PINs, patterns),
- some methods requires some kind of information that user have to remember.

Existing solutions

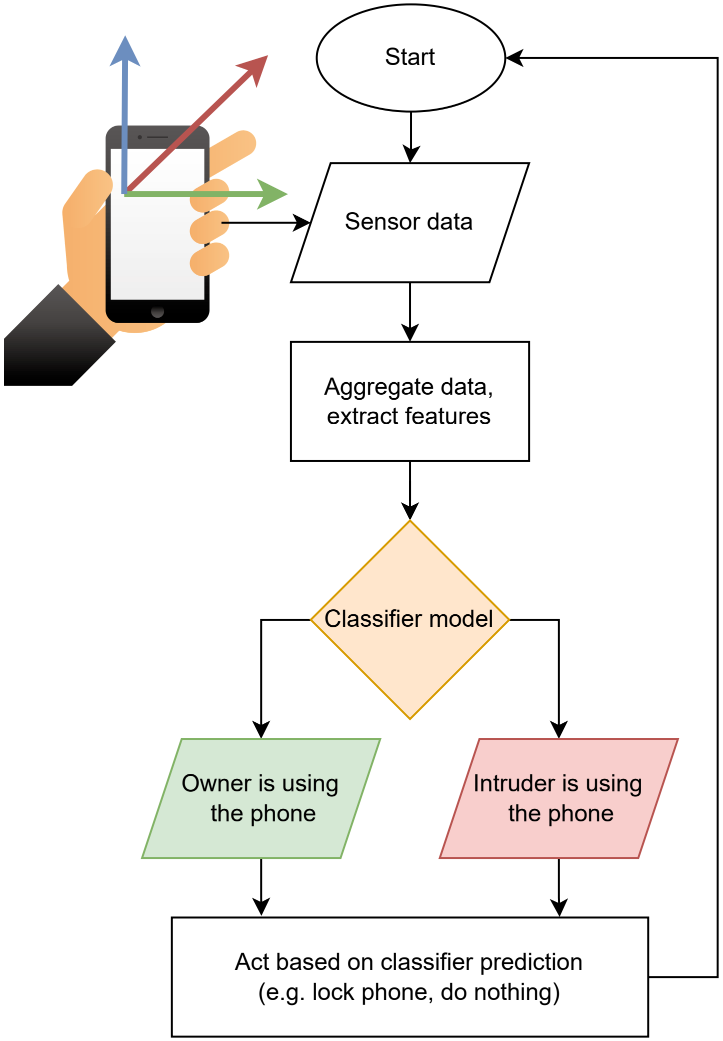
There are many existing articles that examines continuous authentication topics, but many from them:

- require special privileges (cannot be used on normal device),
- require additional special sensors,
- test performance only on computers, not mobile devices,
- don’t examine enrollment process on real mobile devices.

Related work

- A. Buriro, B. Crispo, and Y. Zhauniarovich, “Please hold on: Un-obtrusive user authentication using smartphone’s built-in sensors”, in 2017 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA), 2017, pp. 1–8.
- M. Abuhamad, A. Abusnaina, D. Nyang, and D. Mohaisen, “Sensor-based continuous authentication of smartphones’ users using behavioral biometrics: A contemporary survey”, IEEE Internet of Things Journal, vol. PP, pp. 1–1, 08 2020.
- G. Li and P. Bours, “A novel mobile phone application authentication approach based on accelerometer and gyroscope data”, in 2018 International Conference of the Biometrics Special Interest Group (BIOSIG), 2018, pp. 1–4.
- G. Canfora, P. Di Notte, F. Mercaldo, and C. A. Visaggio, “Silent and continuous authentication in mobile environment”, in SECRYPT, 2016, pp. 97–108.
- Y. Liang, S. Samtani, B. Guo, and Z. Yu, “Behavioral biometrics for continuous authentication in the internet-of-things era: An artificial intelligence perspective”, IEEE Internet of Things Journal, vol. 7, no. 9, pp. 9128–9143, 2020.
- …

Continuous authentication concept



Start

Sensor data

Aggregate data, extract features

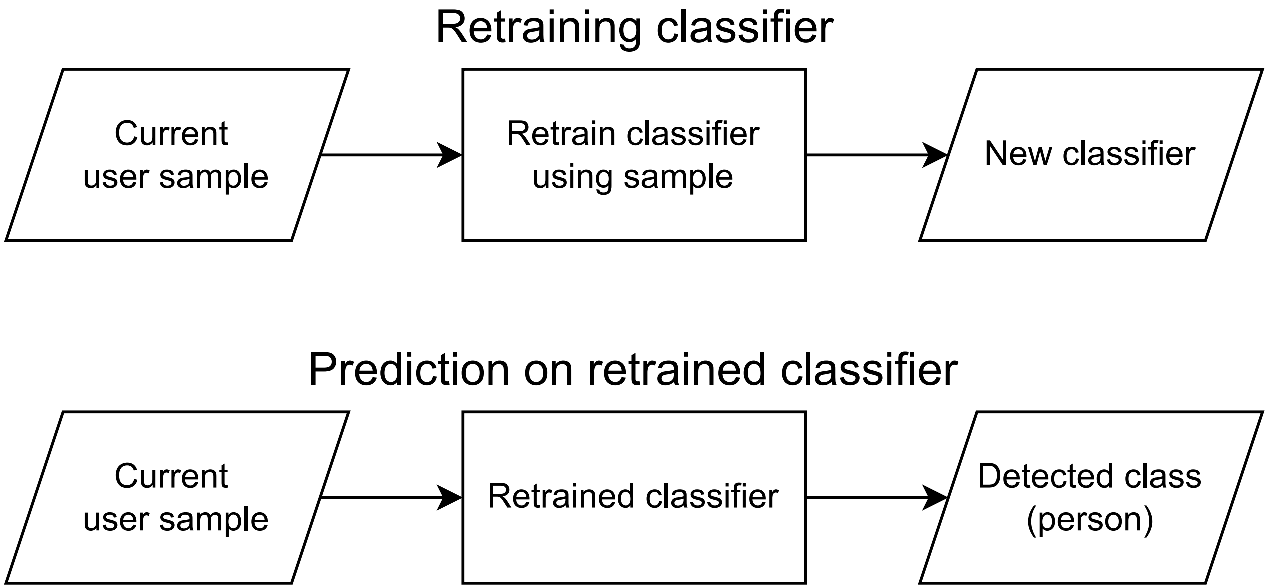
Classifier model

Owner is using the phone

Intruder is using the phone

Act based on classifier prediction (e.g. lock phone, do nothing)

First approach – model based

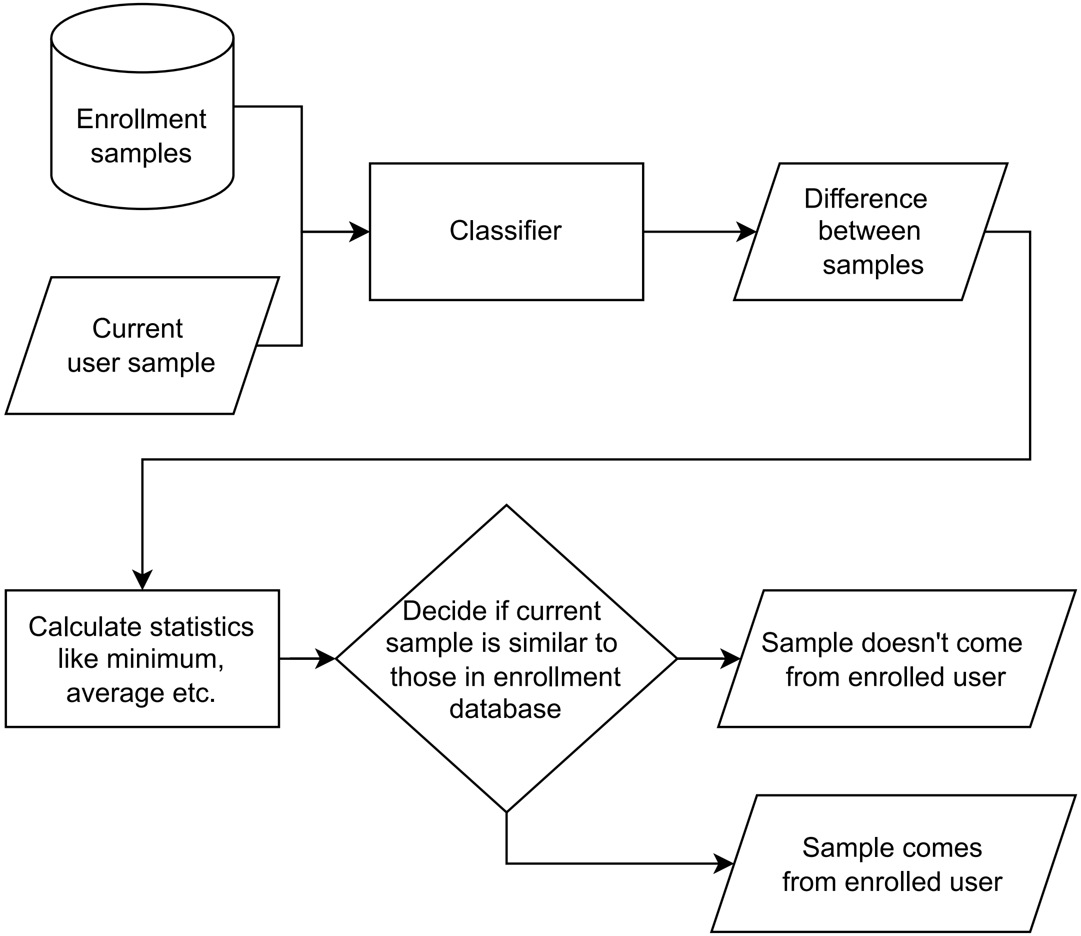

Retraining classifier

Current user sample → Retrain classifier using sample → New classifier

Prediction on retrained classifier

Current user sample → Retrained classifier → Detected class (person)

Second approach – template based

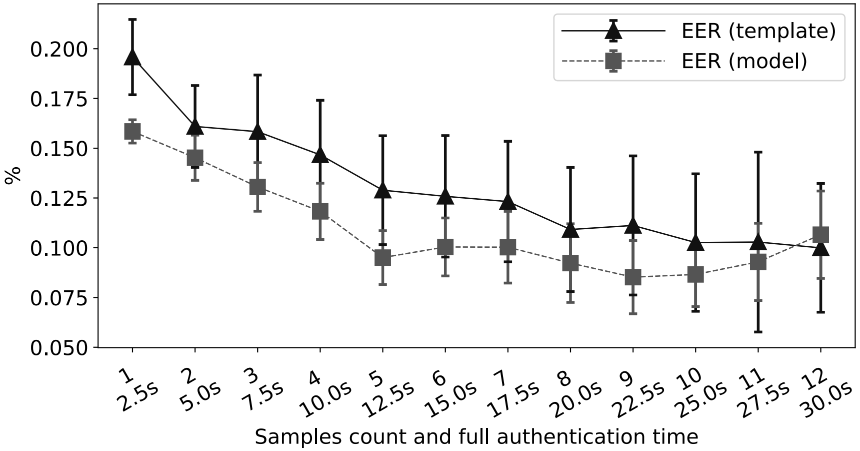

Enrollment samples
Current user sample
Classifier
Difference between samples
Calculate statistics like minimum, average etc.
Decide if current sample is similar to those in enrollment database
Sample doesn't come from enrolled user
Sample comes from enrolled user

Experiments

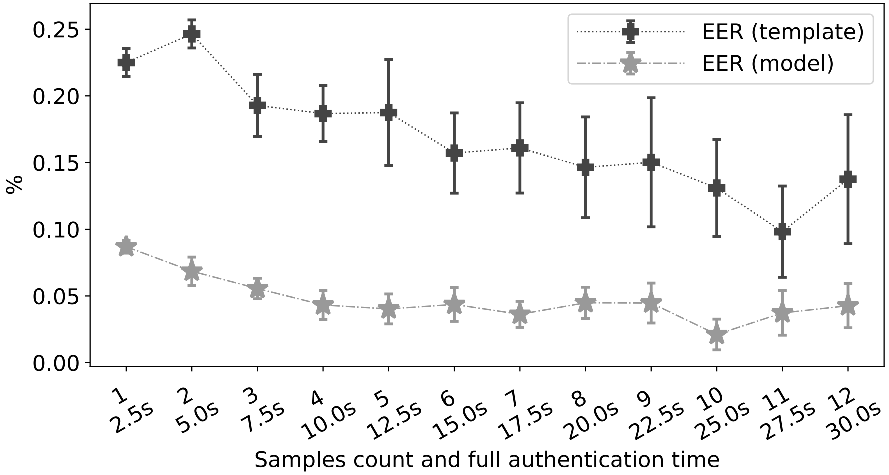
- 5 people
- 200 minutes of data from sensors
- two approaches: model and template based
- enrollment and performance considered

Results

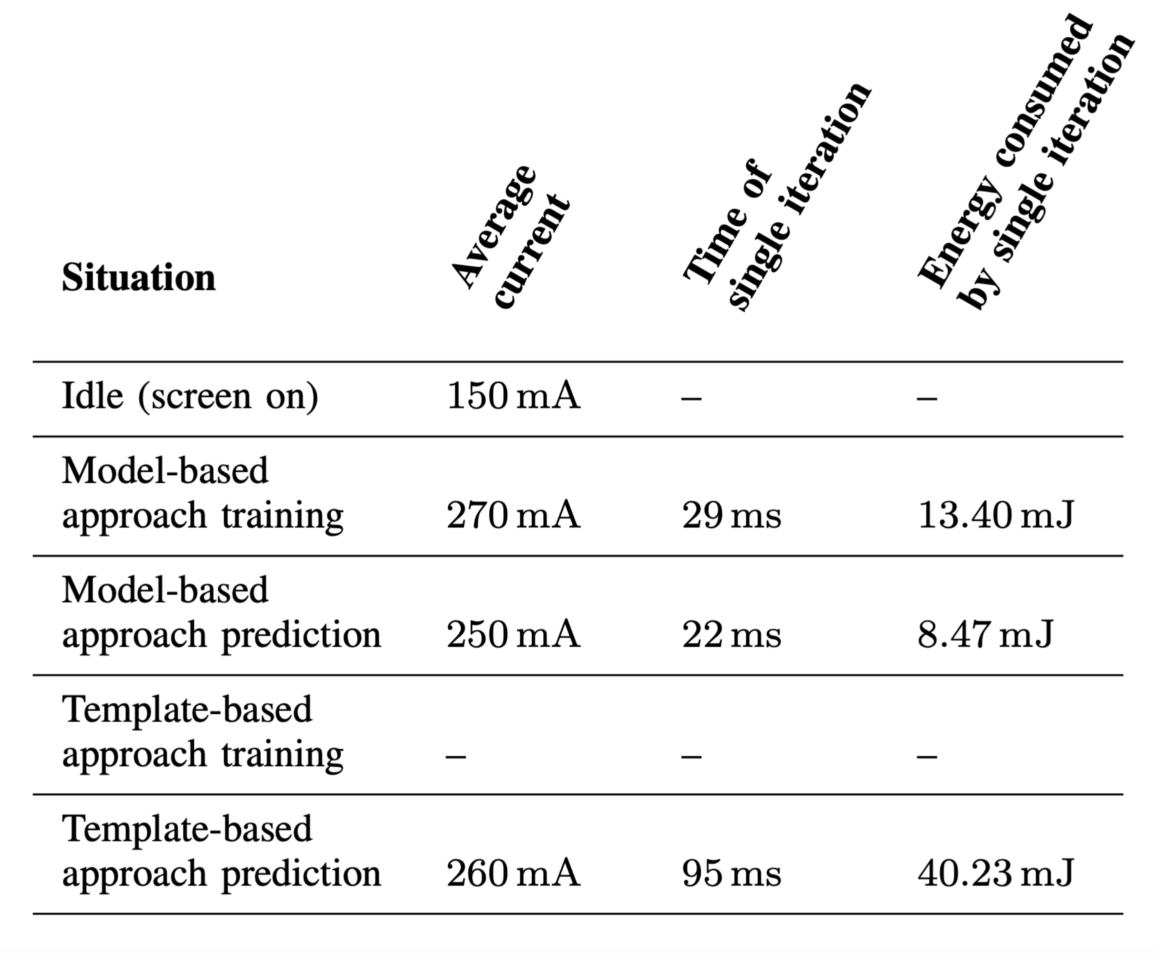
EER graph



EER graph (new user)



Results – performance



Situation	Average current	Time of single iteration	Energy consumed by single iteration
Idle (screen on)	150 mA	–	–
Model-based approach training	270 mA	29 ms	13.40 mJ
Model-based approach prediction	250 mA	22 ms	8.47 mJ
Template-based approach training	–	–	–
Template-based approach prediction	260 mA	95 ms	40.23 mJ

Summary

- most of existing articles about continuous authentication don’t take up the topic of on-device enrollment,
- combination of static and continuous authentication can improve security,
- template-based approach, while having worse accuracy, can temporarily work almost instantly when model is being built for the user,
- tests also showed that today’s smartphones are capable of on-device training, but there are concerns about time of such training and battery consumption.

Thank you!