

Behavioural Biometrics-Based User Authentication

Andraž Krašovec, Ispra, 11.5.2022
andraz.krasovec@ec.europa.eu

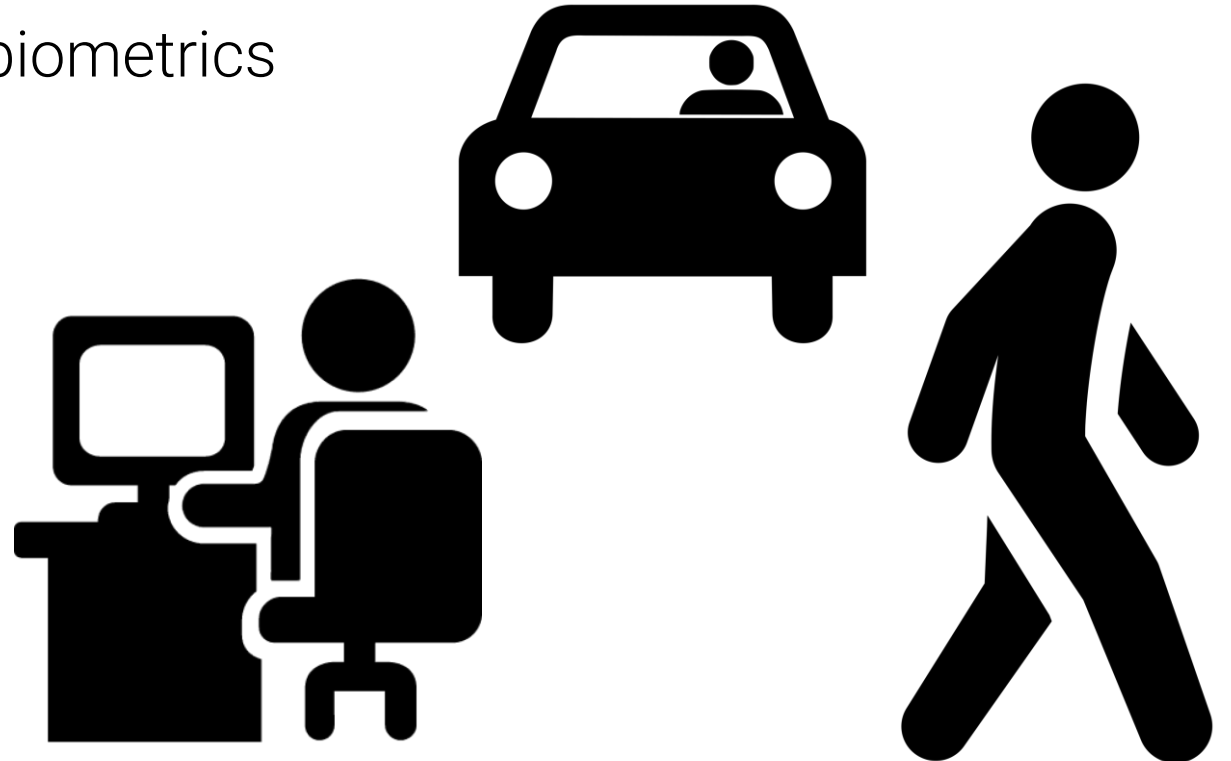


Univerza v Ljubljani
Fakulteta *za računalništvo*
in informatiko



Towards Password-less Authentication

- Current user authentication methods have many shortcomings
 - Frustration handling passwords
 - Privacy concerns of physical biometrics
 - User is an active component
- Behavioural biometrics:
 - Convenient
 - Multimodal
 - Privacy oriented



Identification, Authentication, Authorisation

The image shows a Facebook login interface. On the left, the Facebook logo and a tagline are displayed. On the right, there is a login form with two input fields: 'Email or phone number' and 'Password'. Below these fields is a blue 'Prijava' (Login) button. A link 'Se ne spomniš gesla?' (Don't remember your password?) is located below the login button. At the bottom of the form is a green 'Ustvari nov račun' (Create new account) button. Three arrows are overlaid on the image: an orange arrow points from the top left towards the 'Email or phone number' field (representing Identification); a yellow arrow points from the top center towards the 'Password' field (representing Authentication); and a green arrow points from the top right towards the 'Prijava' button (representing Authorisation).

facebook

Facebook ti pomaga ohranjati stike in deliti podatke z ljudmi iz tvojega življenja.

Email or phone number

Password

Prijava

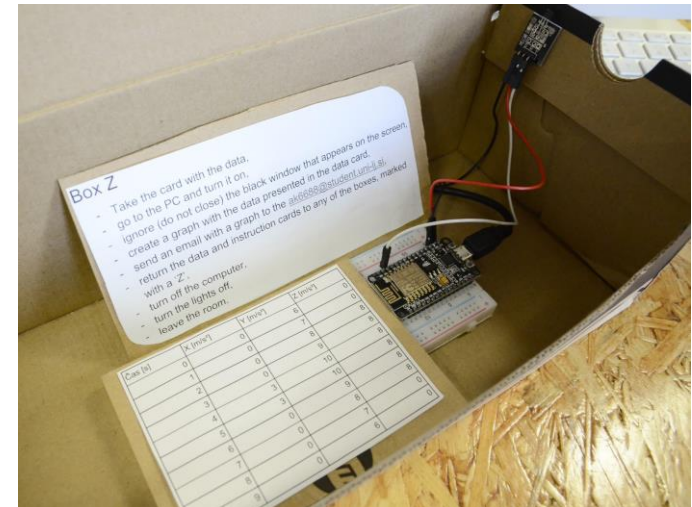
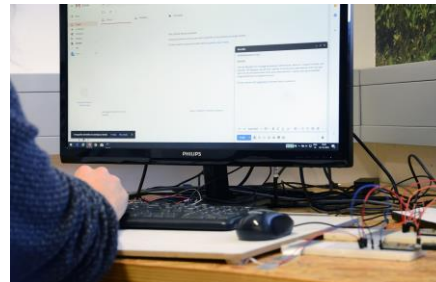
[Se ne spomniš gesla?](#)

Ustvari nov račun

Not Quite Yourself Today: Behaviour-Based Continuous Authentication in IoT Environments

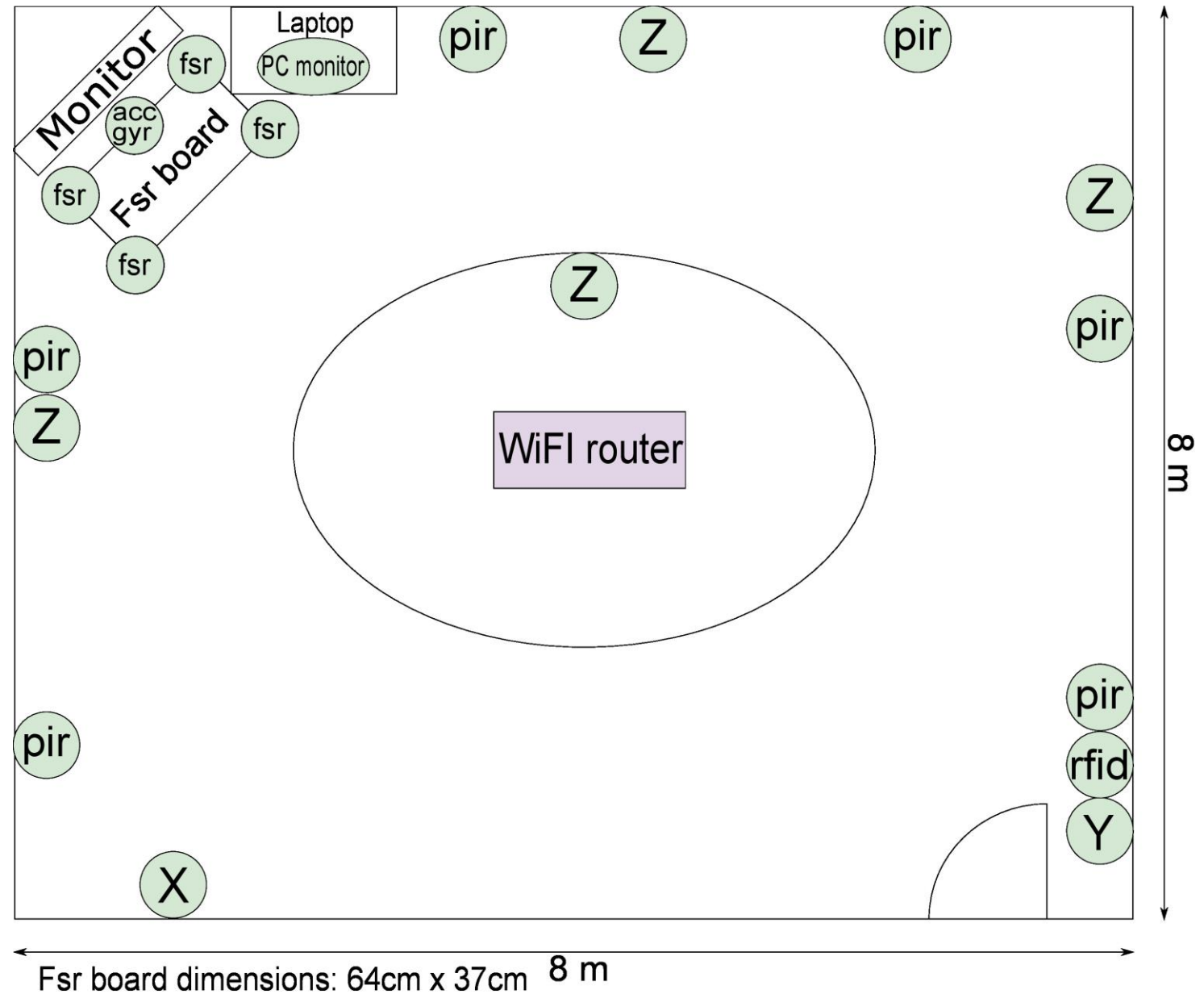
User Study

- 21 test subjects
- 3 experimental tasks
- 2 runs per task
- ~1 hour of data per person
- Tasks stimulate responses from different sensors



Environment

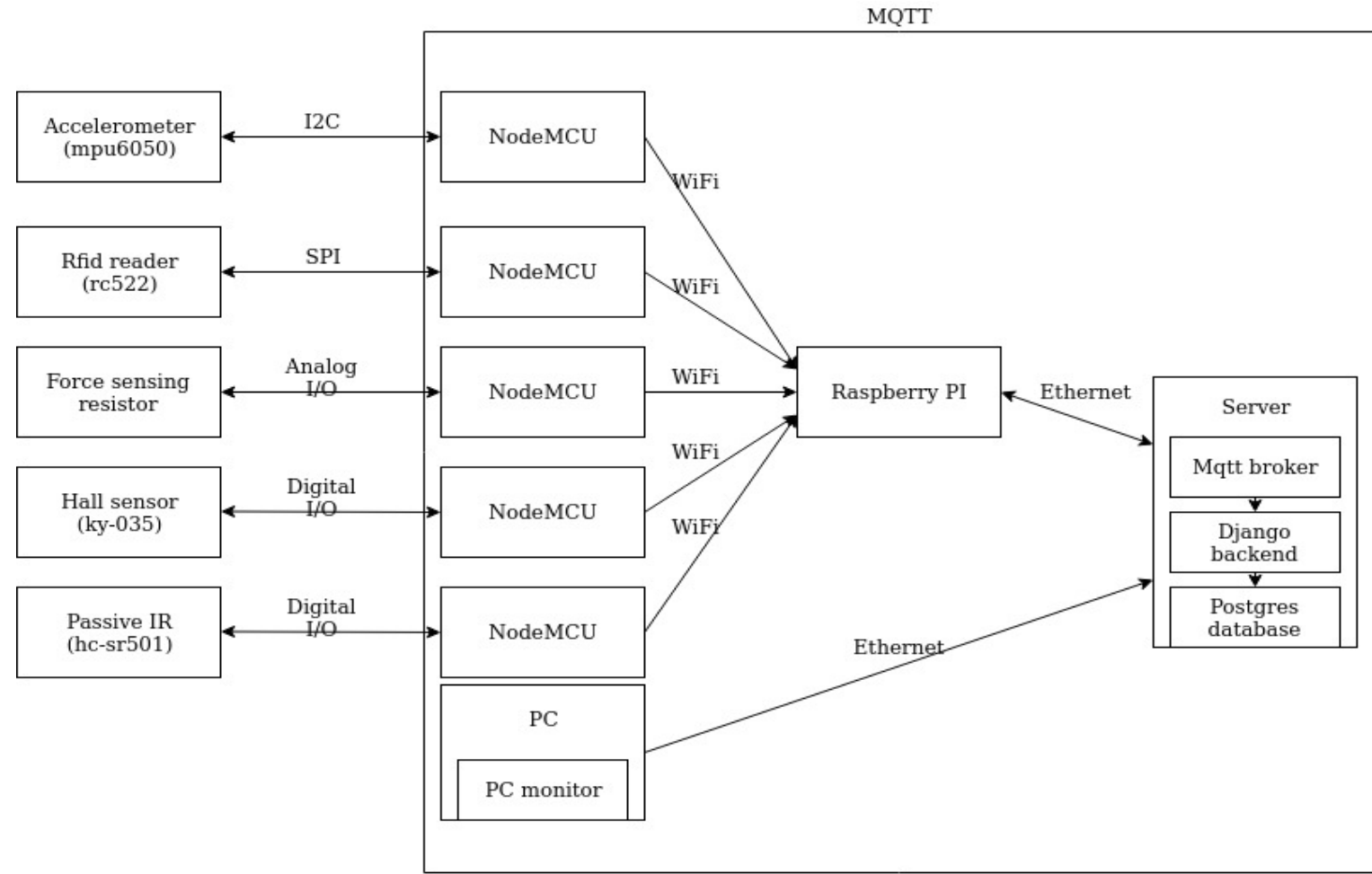
- Office space
- PC resource monitor
- 6-axis IMU
- Force sensors
- IR sensors
- Hall sensors



Data Collection Architecture

Low cost solution

- Arduino-based
- ESP 8266
- Rpi router
- Low spec server



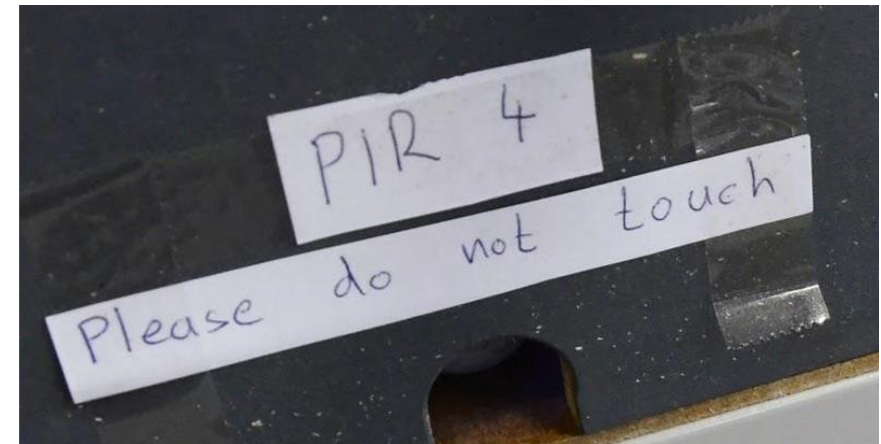
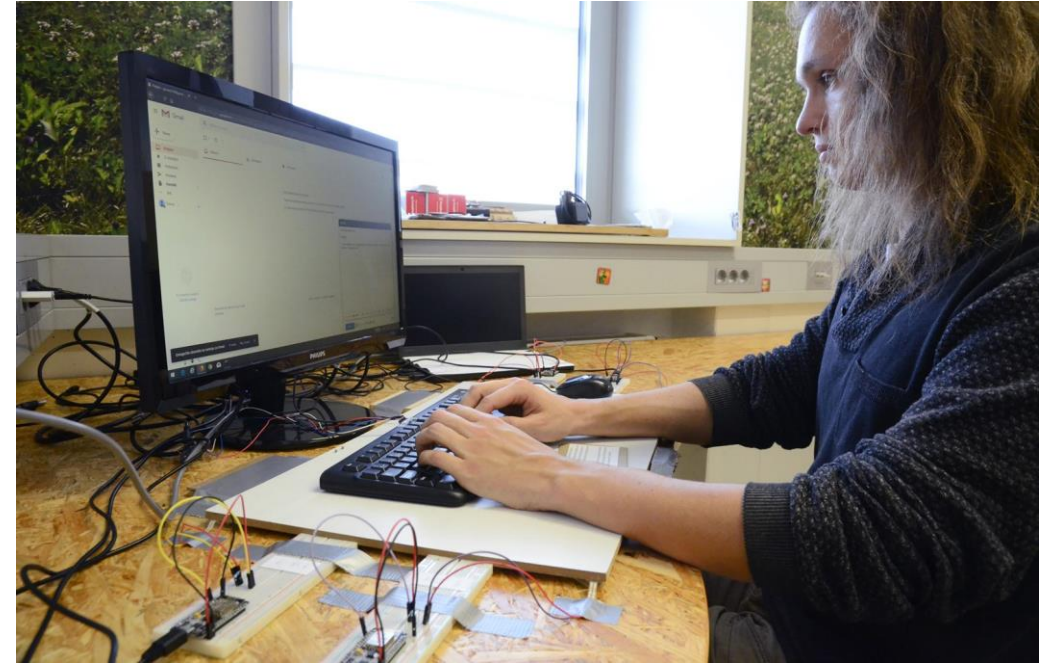
Data Collection Architecture

- Django framework
- PostgreSQL database
- MQTT protocol + Mosquitto broker
- RabbitMQ message broker
- Custom deployment software

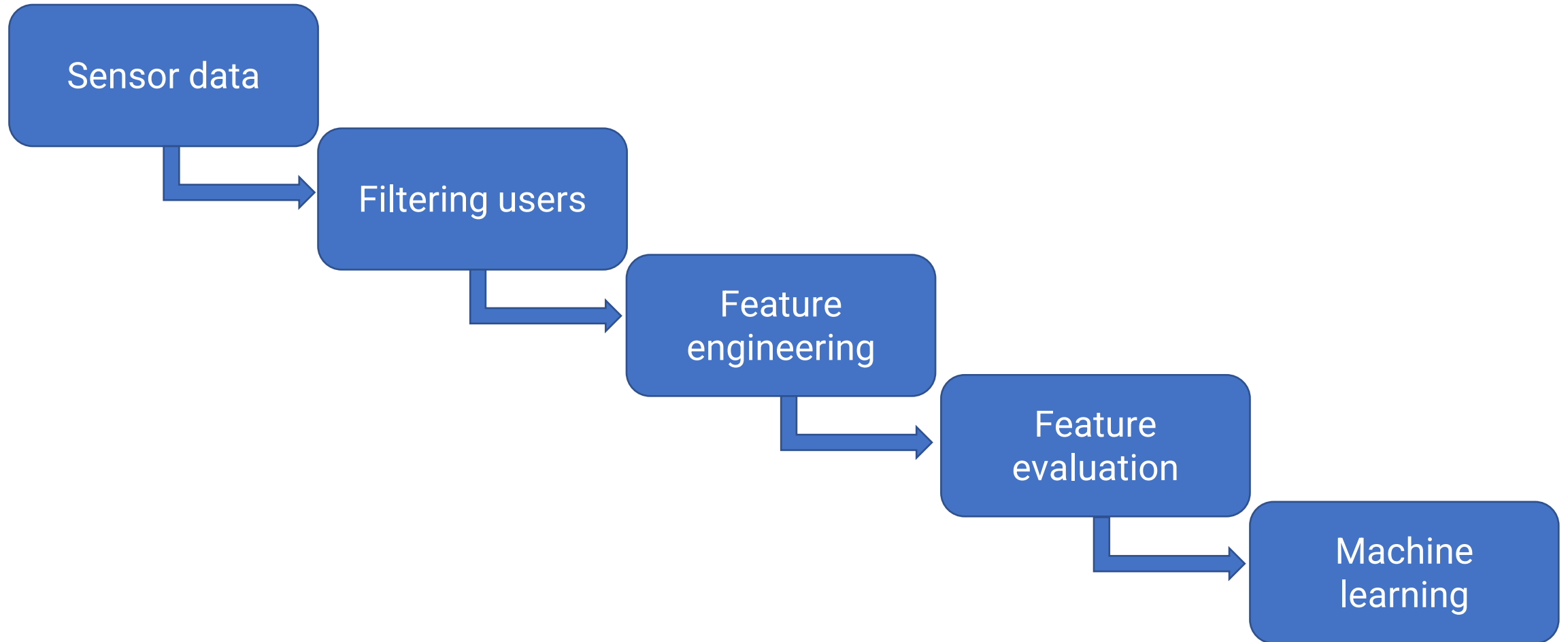
Topic	Publisher	Subscriber	Name	Message type	Description
data/{device_id}/{sensor_topic}	Devices	Data manager	Data	float	Send sensor values to be stored in db.
command/{device_id}/{command}	Device manager, Seance manager	Devices	Command	string	Issue commands to devices.
configure/{device_id}/{command}	Devices	Device manager	Configure	string	Receive commands from devices.
seance/{device_id}/{command}	Device rc522	Seance manager	Seance	string	Used to indicate seance state.

Challenges

- Supplying power
- Fragile sensor connections
- Sampling rate
- Data ingestion rate
- RFID reader
- Users copying text between runs
- Users not following instructions
- Shared space – equipment borrowing

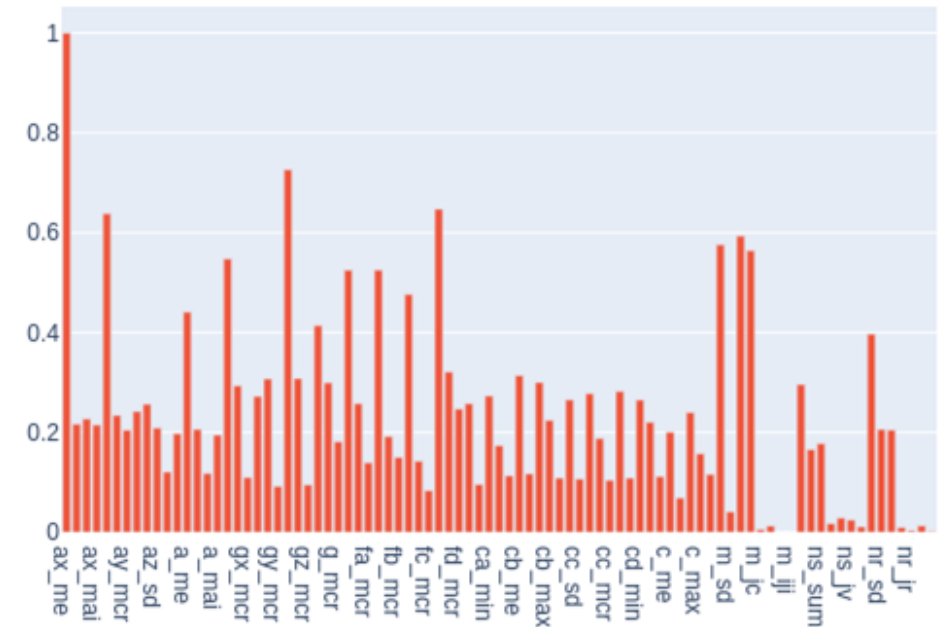


Machine Learning Pipeline



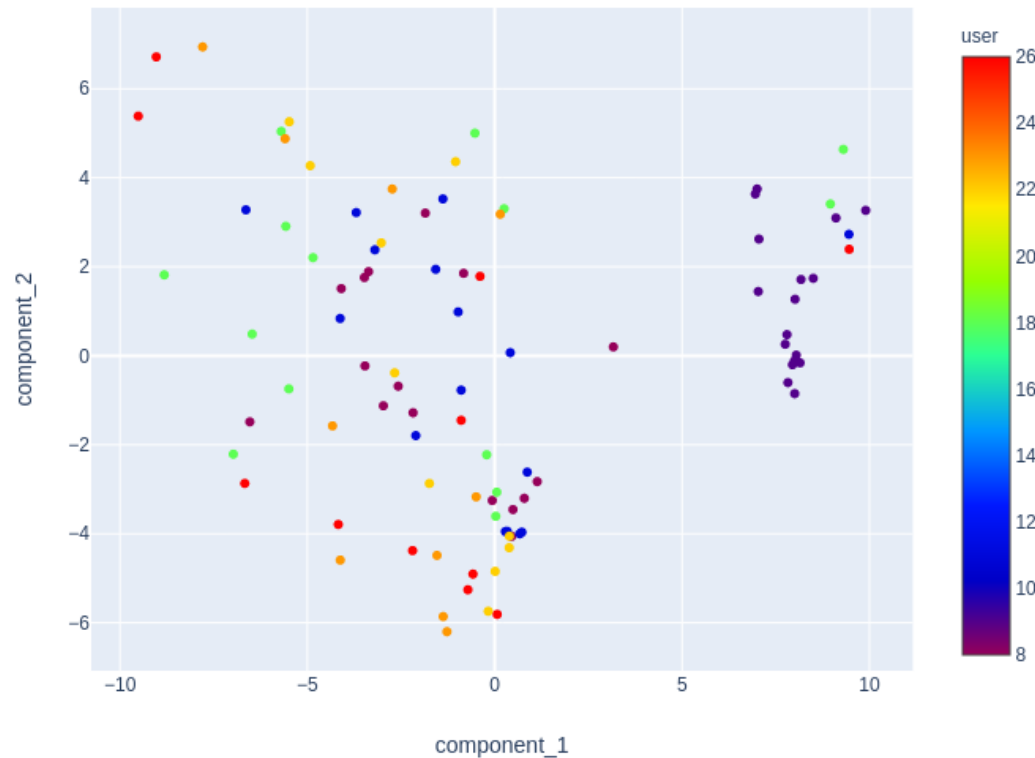
Feature Engineering

- Segmenting data into time intervals
- Time domain features
- Frequency domain features
- Evaluating feature quality
- Autoencoders?

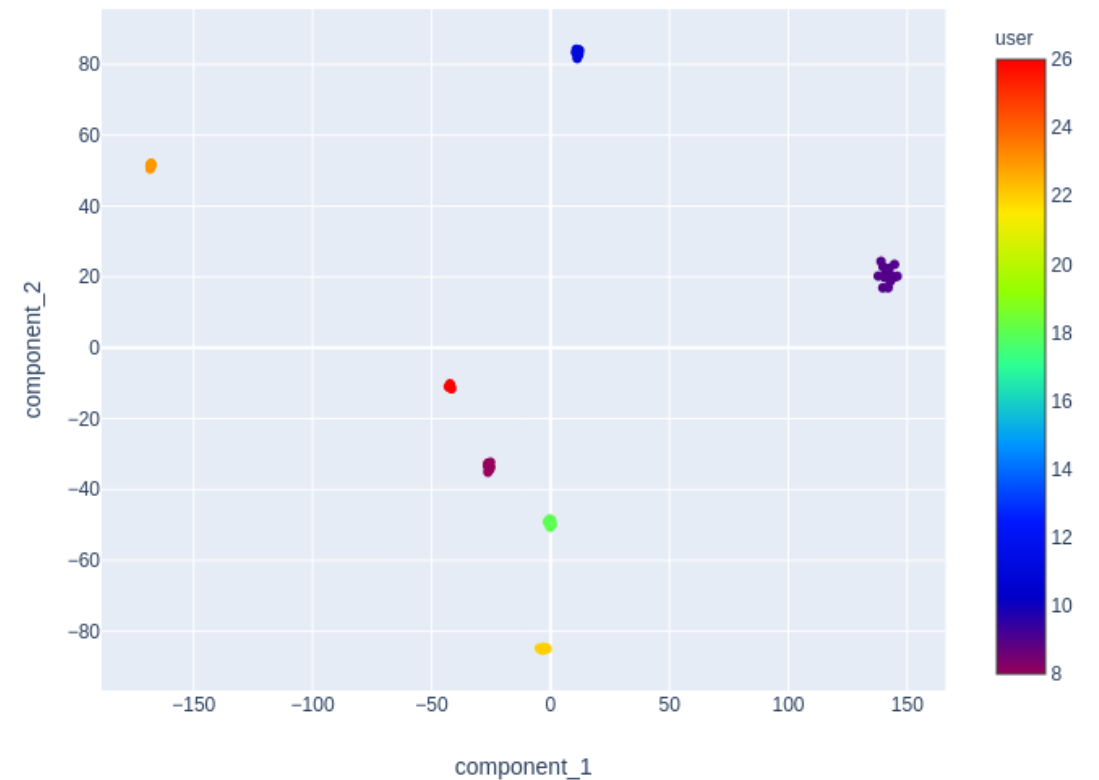


Preliminary Data Analysis

PCA TECHNIQUE; number of users: 7, segment interval: 60 seconds, score: 10.0

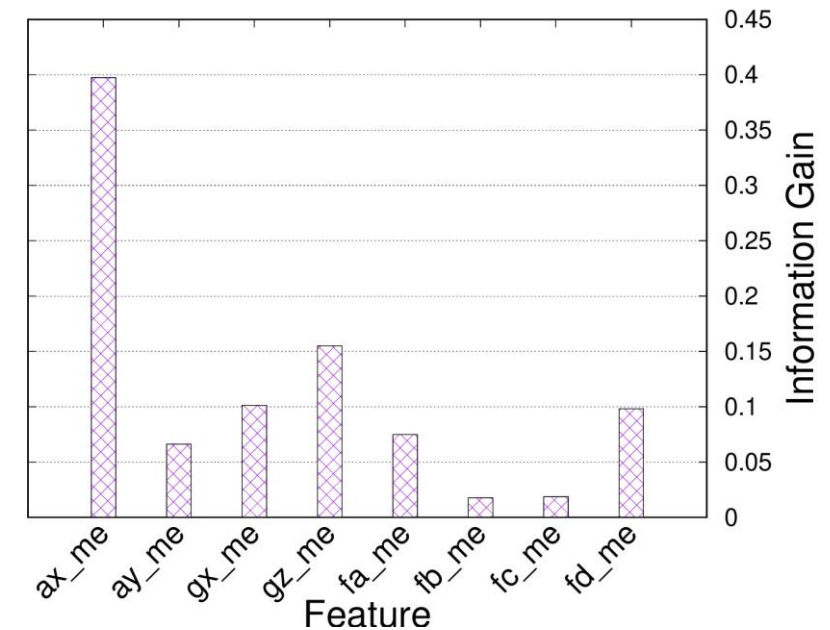
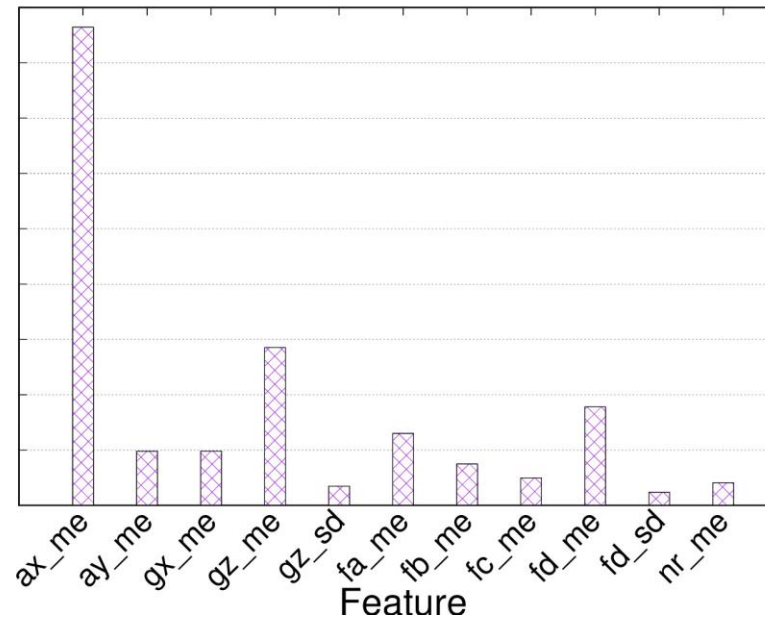
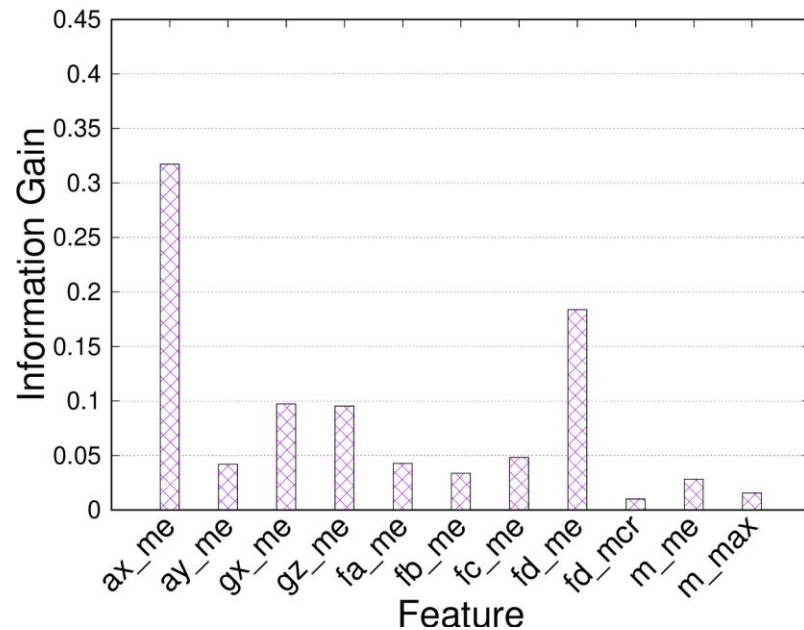


LDA TECHNIQUE; number of users: 7, segment interval: 60 seconds, score: 77136.0



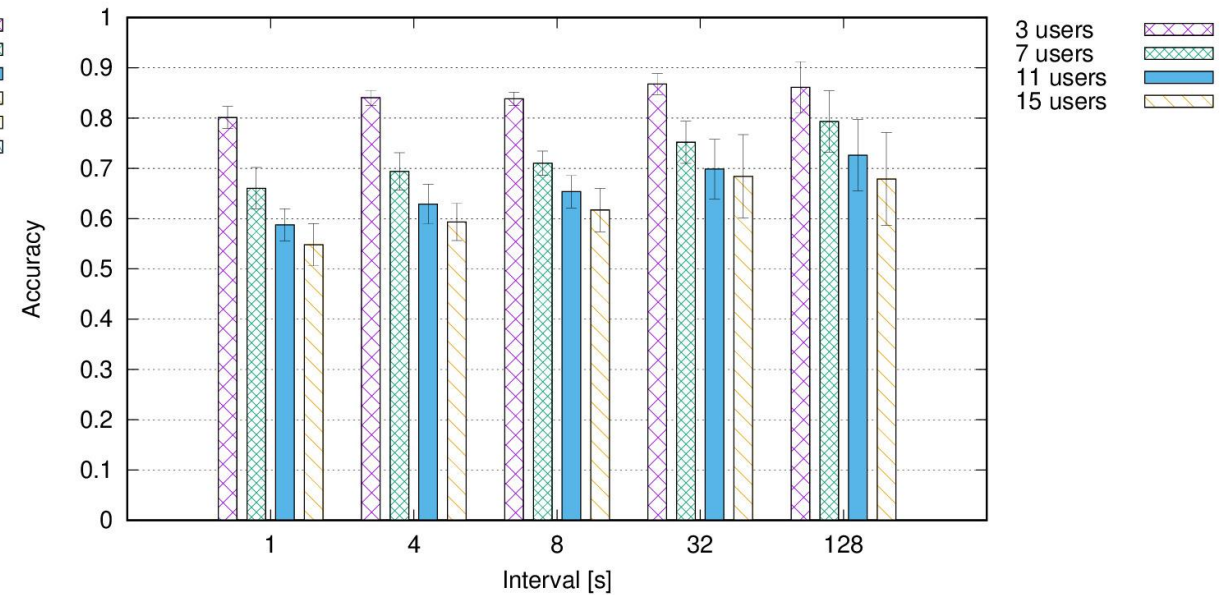
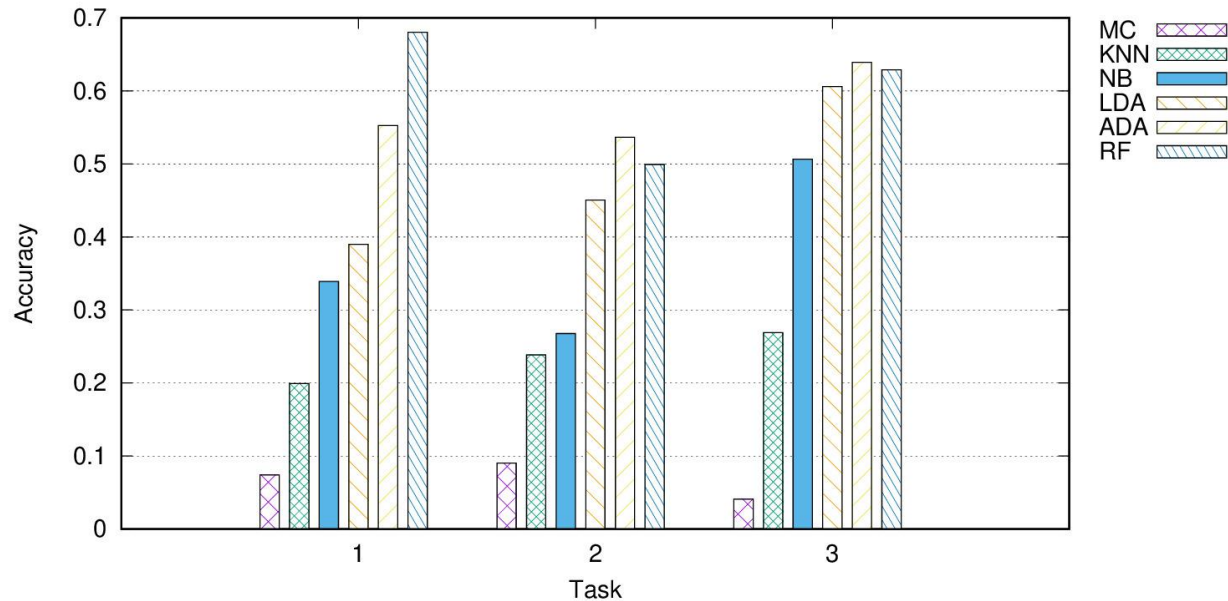
Sensor and Feature Informativeness

- Inertial measurement unit and force sensors perform best



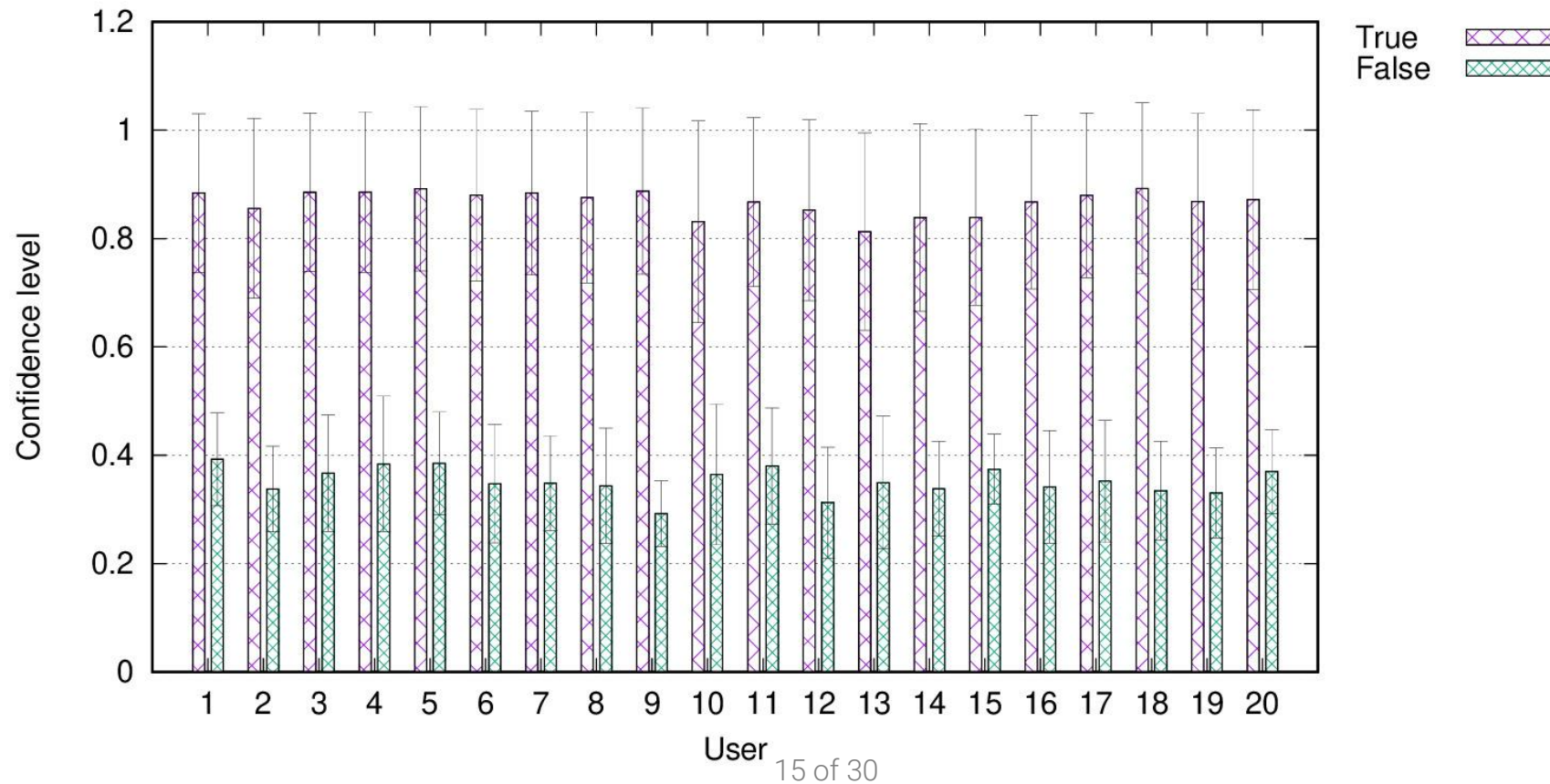
One-shot Authentication

- Comparison of machine learning algorithms
- Effect of number of users and time segment intervals
- Can we replace passwords?



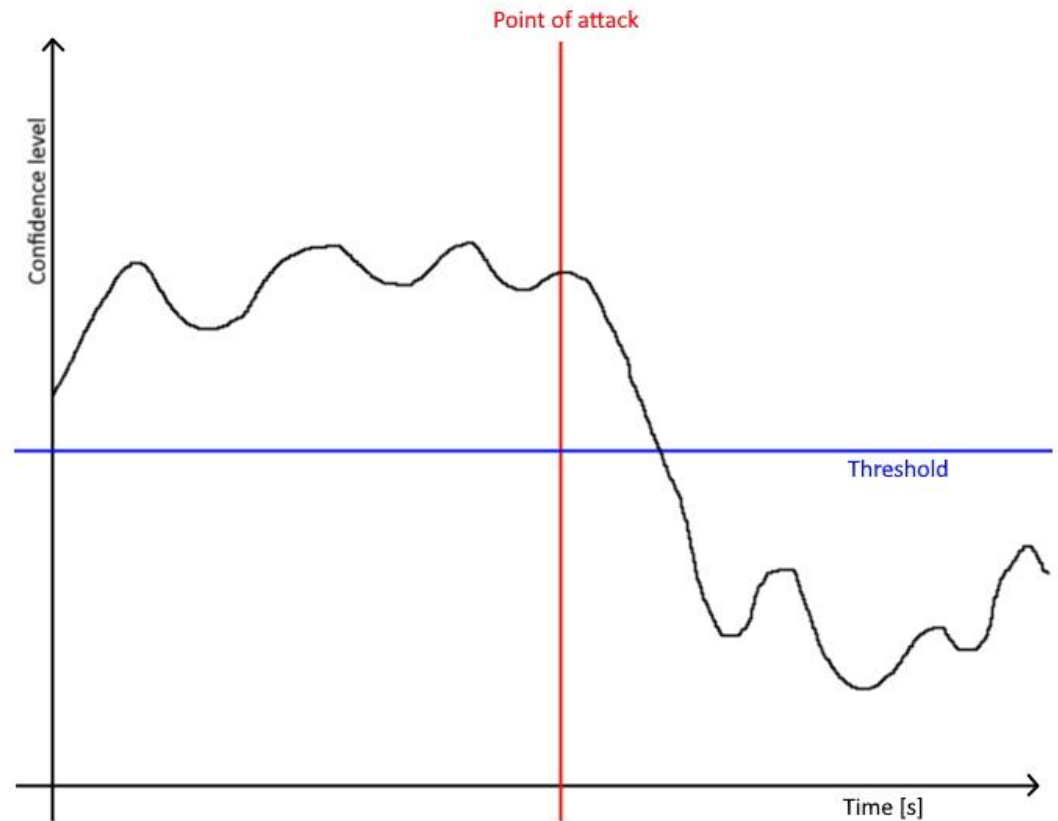
Transition to Continuous Authentication

Difference between true and false confidence



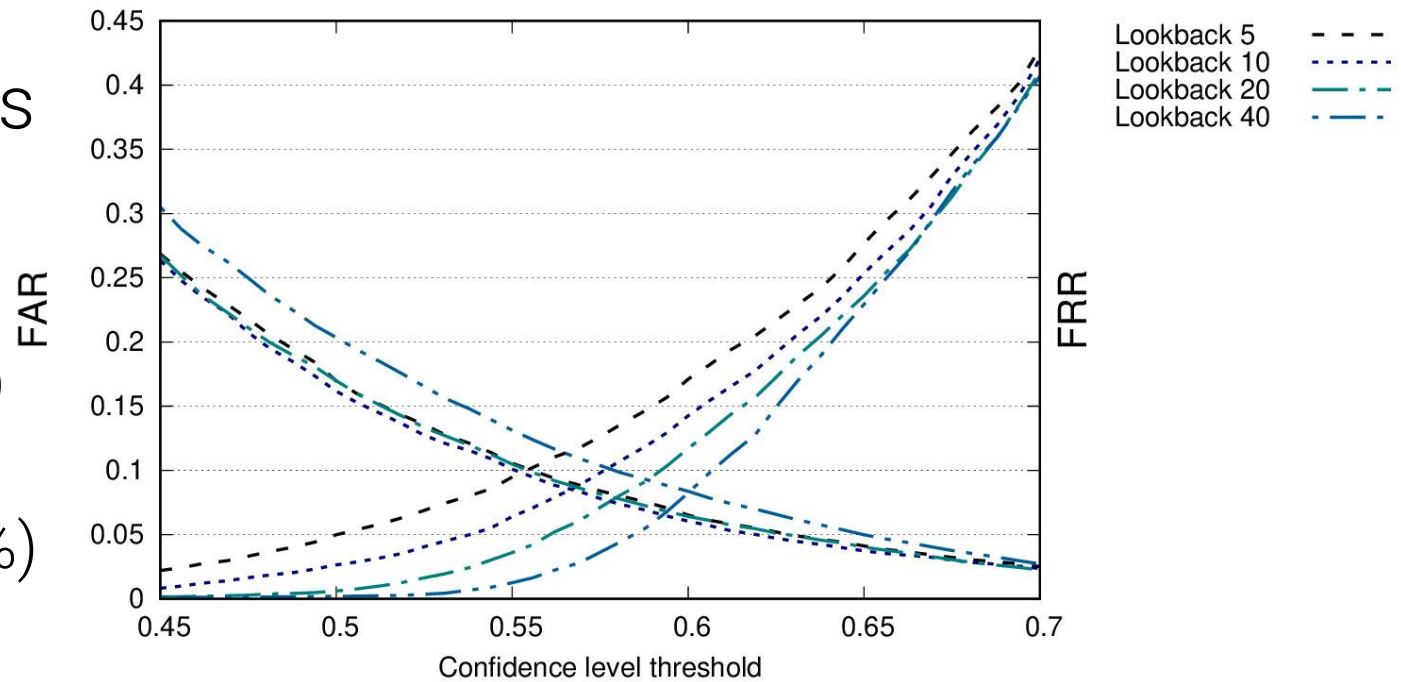
Continuous Authentication

- Confidence level threshold
- n (lookback) last datapoints
- Evaluation metrics:
 - False rejection rate (FRR)
 - False acceptance rate (FAR)
 - Detection time delay
 - Attack detection rate (99.3%)



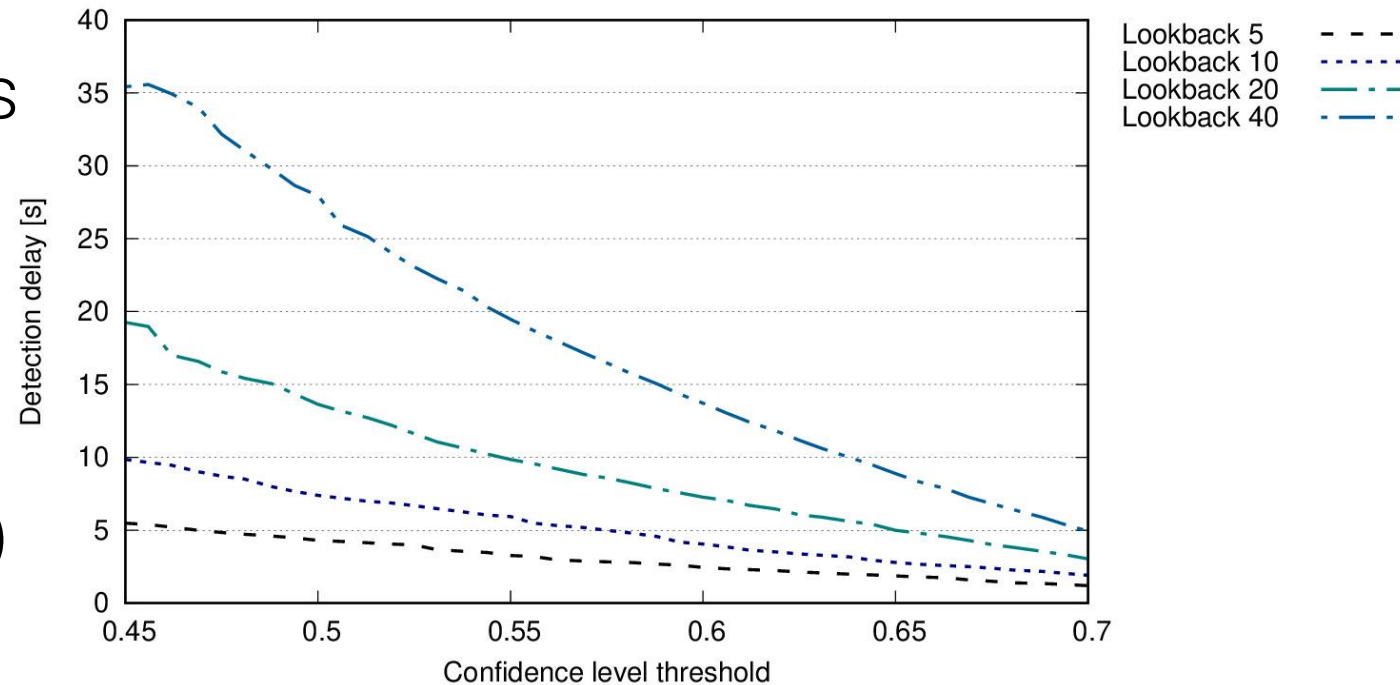
Continuous Authentication

- Confidence level threshold
- n (lookback) last datapoints
- Evaluation metrics:
 - False rejection rate (FRR)
 - False acceptance rate (FAR)
 - Detection time delay
 - Attack detection rate (99.3%)



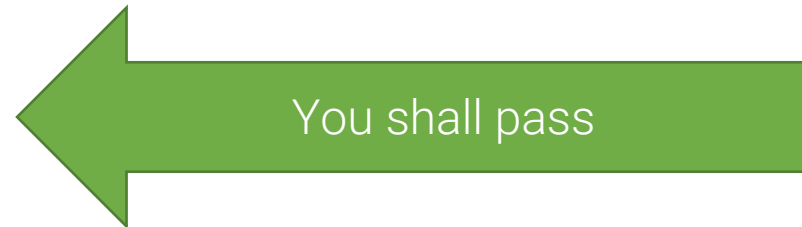
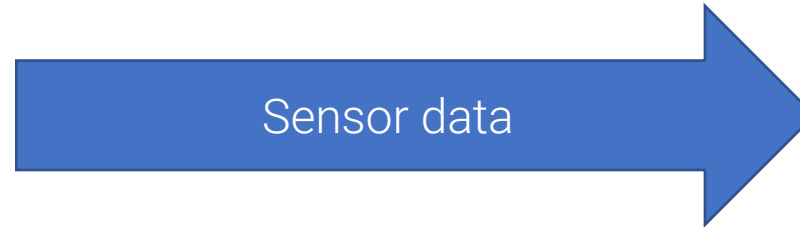
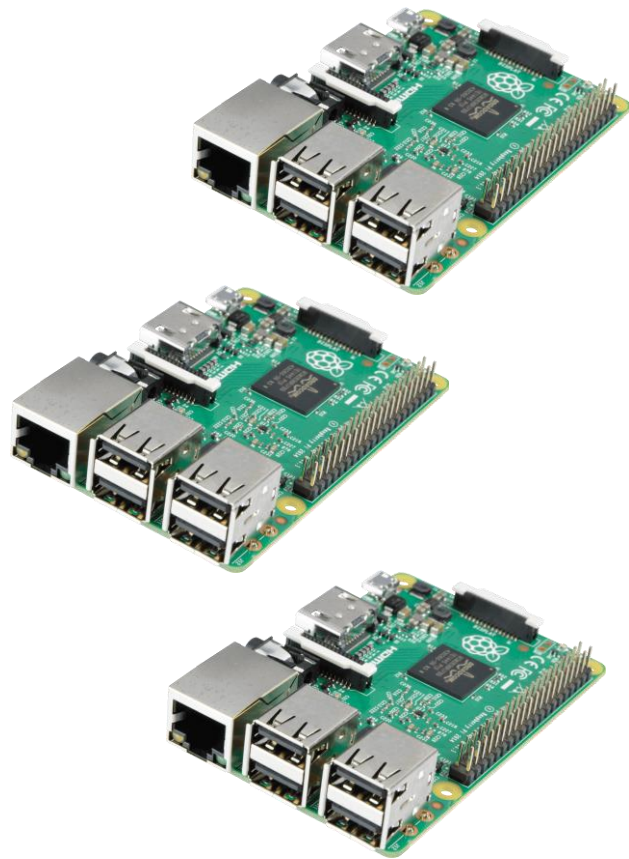
Continuous Authentication

- Confidence level threshold
- n (lookback) last datapoints
- Evaluation metrics:
 - False rejection rate (FRR)
 - False acceptance rate (FAR)
 - Detection time delay
 - Attack detection rate (99.3%)



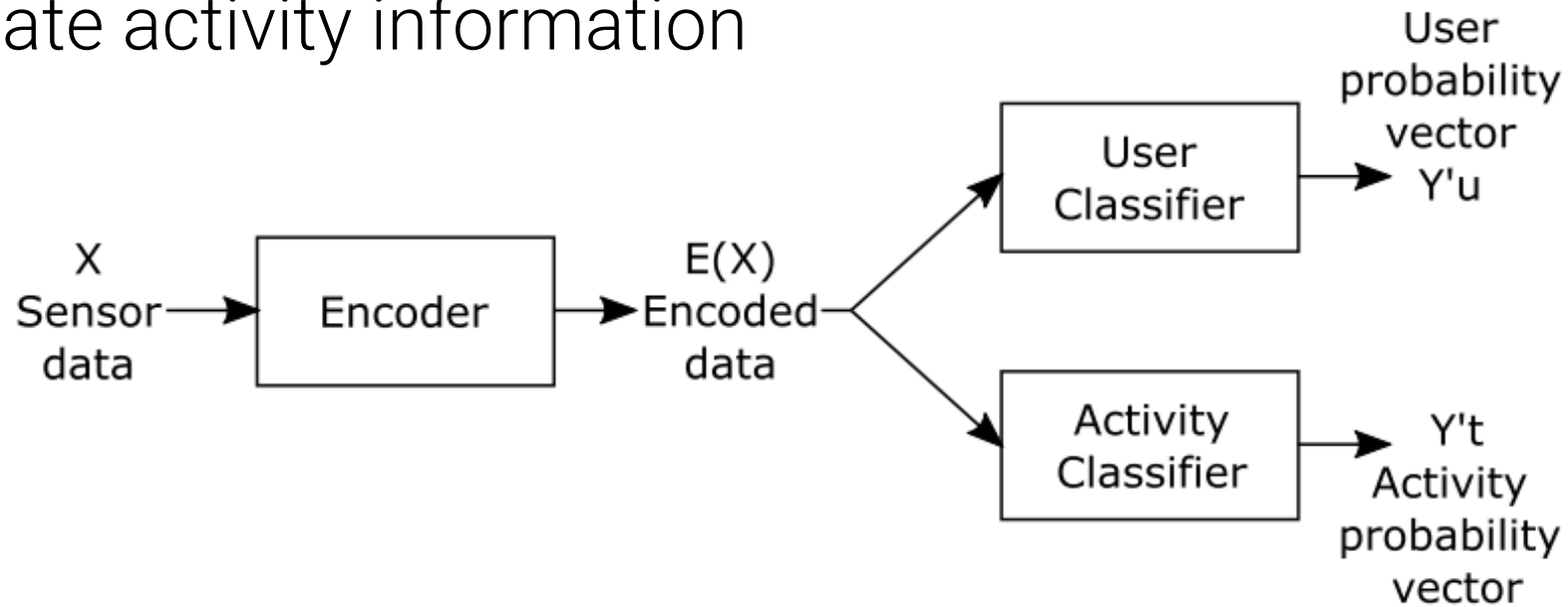
Opposing Data Exploitation: Behaviour Biometrics for Privacy-Preserving Authentication in IoT Environments

Privacy Attack Scenario



System Design

- Based on Privacy Adversarial Network [1]
- Adversarial learning
- Obfuscate activity information

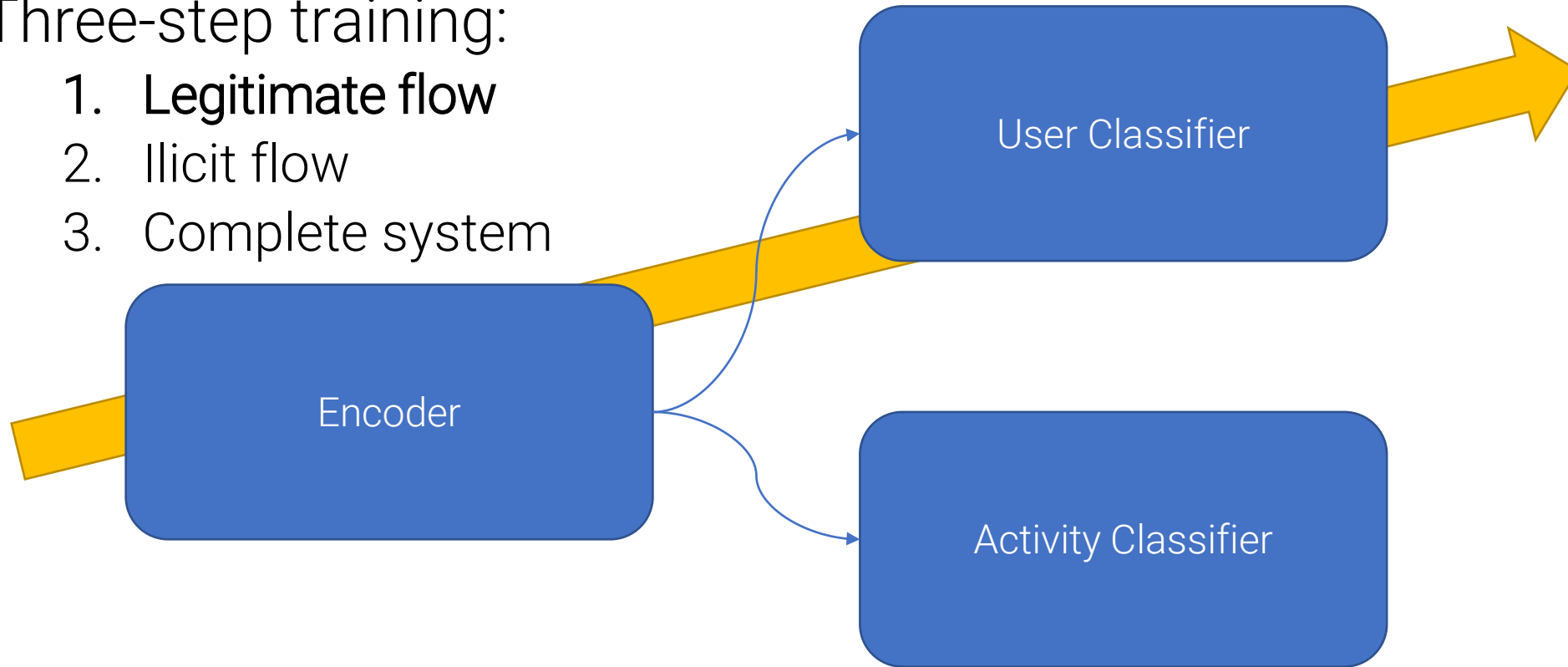


[1] Liu et al.: Privacy Adversarial Network: Representation Learning for Mobile Data Privacy, 2019.

Adversarial Training Algorithm

Three-step training:

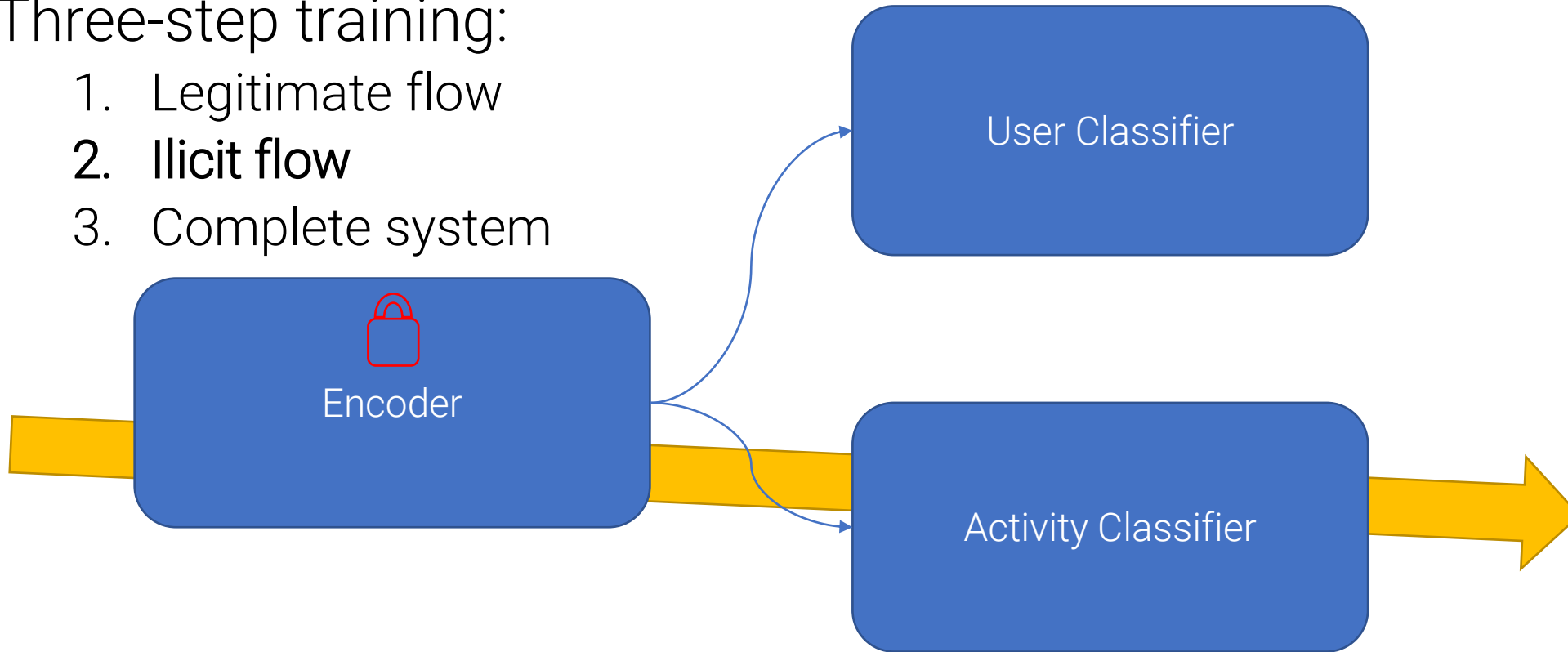
1. Legitimate flow
2. Ilicit flow
3. Complete system



Adversarial Training Algorithm

Three-step training:

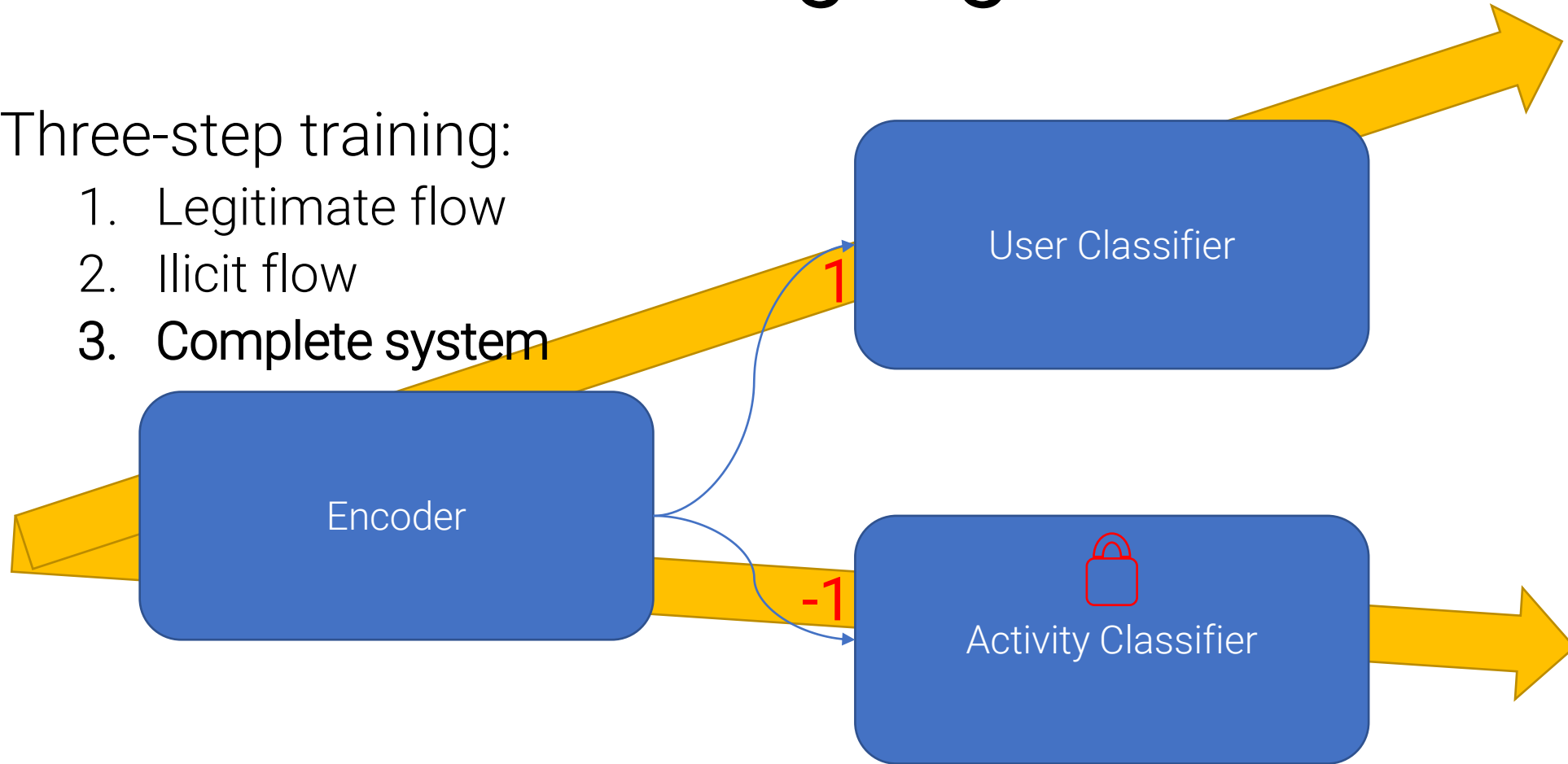
1. Legitimate flow
2. **Ilicit flow**
3. Complete system



Adversarial Training Algorithm

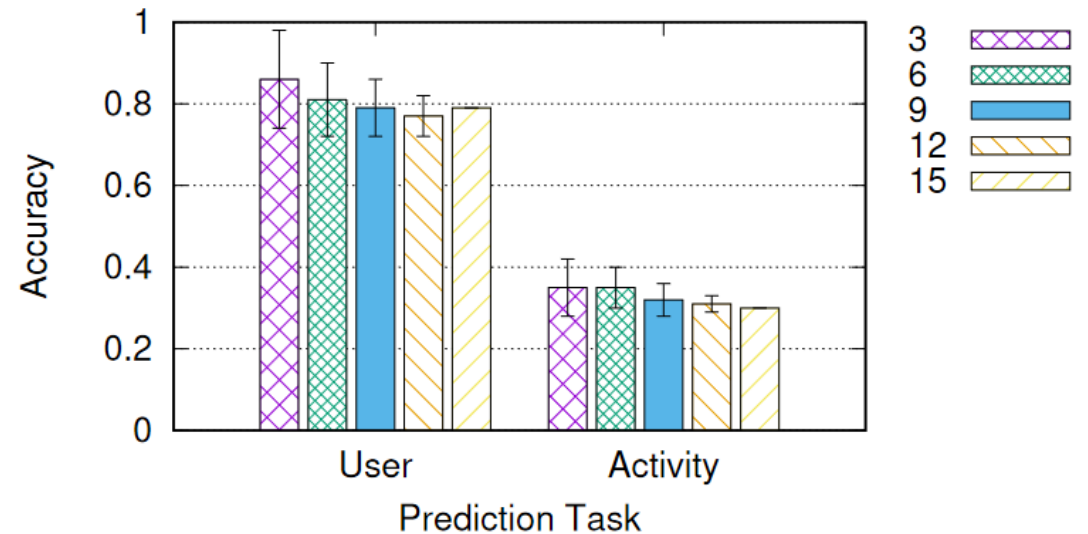
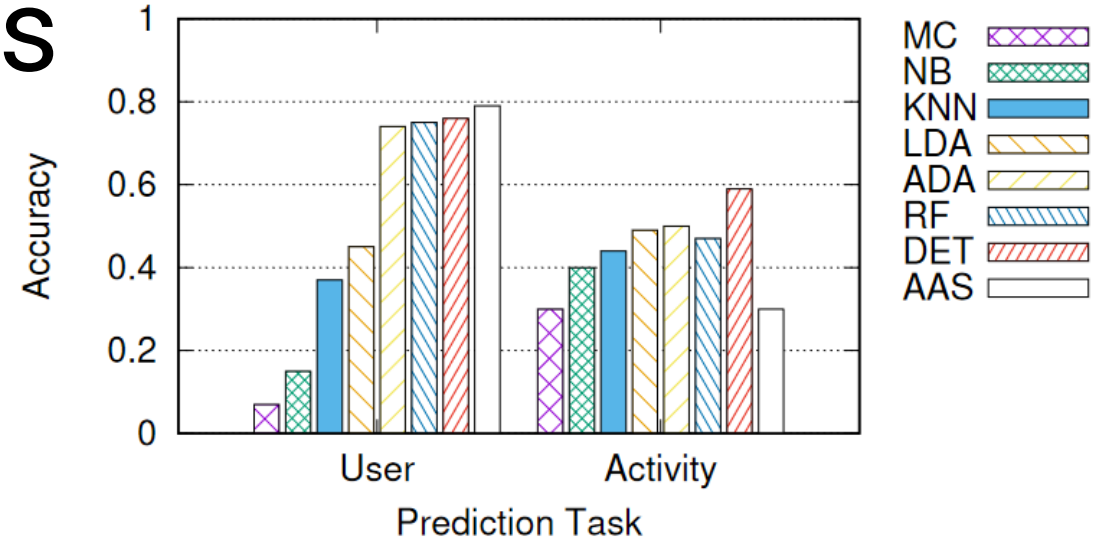
Three-step training:

1. Legitimate flow
2. Ilicit flow
3. Complete system

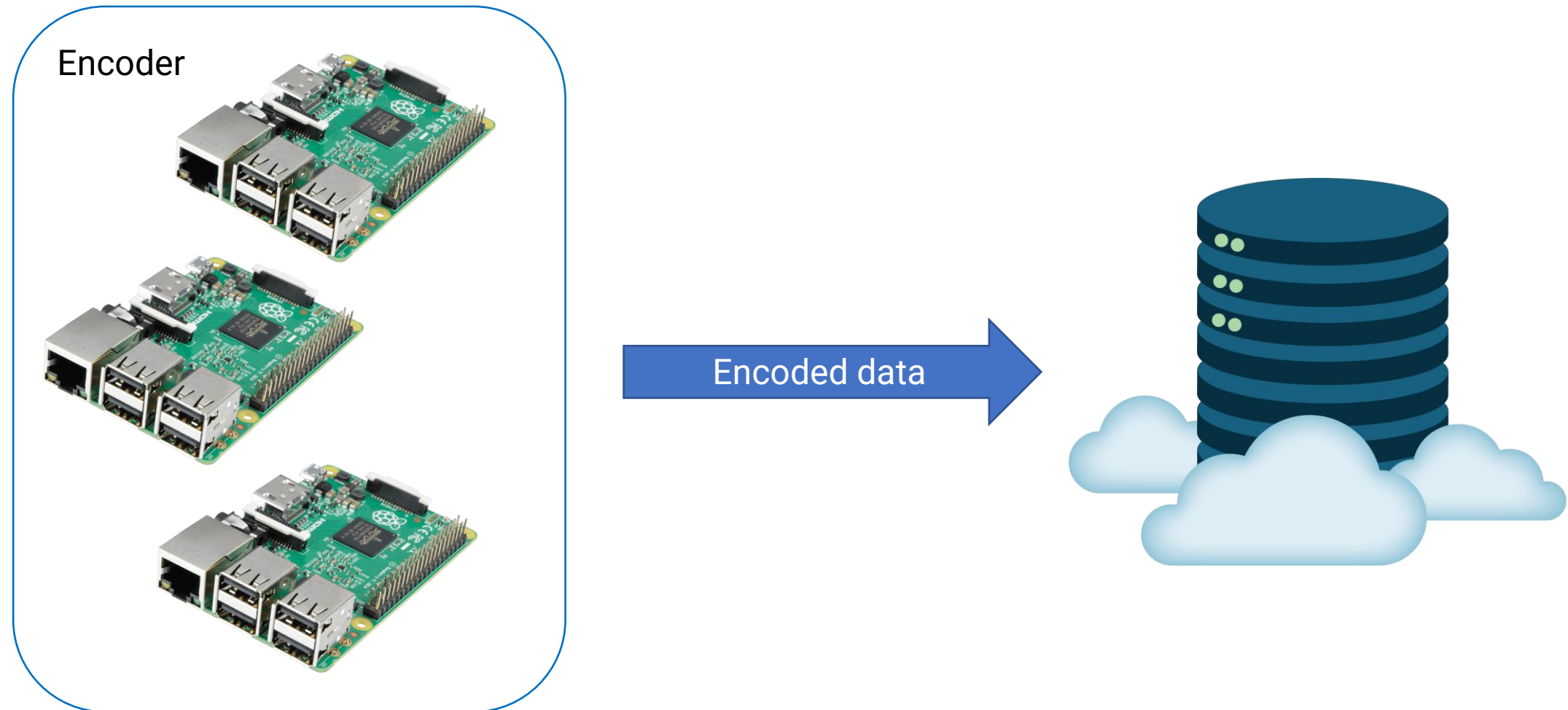


Authentication Results

- 79% user classification accuracy
- 30% reduction in activity classification accuracy
- Inverse problem
- Effect of number of users



On-Device Training Issue

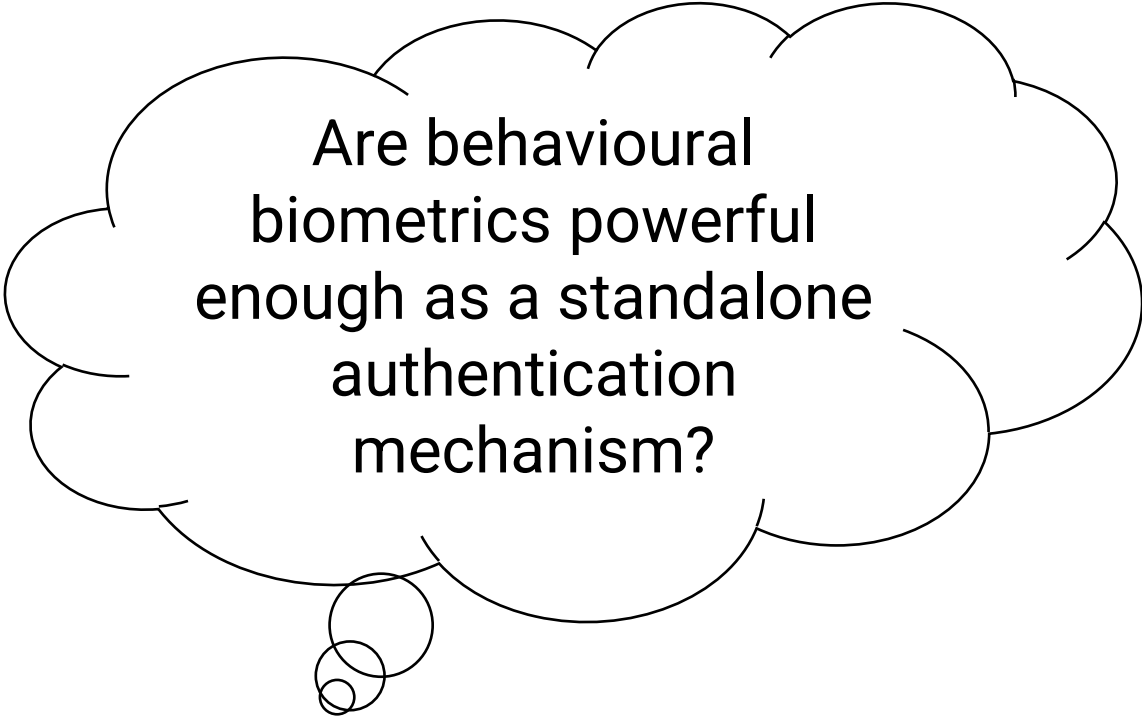


Conclusion

- One-shot authentication with behavioural biometrics is tricky
- Very well suited for continuous authentication

Future work:

- Improving one-shot auth. accuracy
- Focus on cognitive load
- Collecting a new dataset
- Development of auth. evaluation toolbox

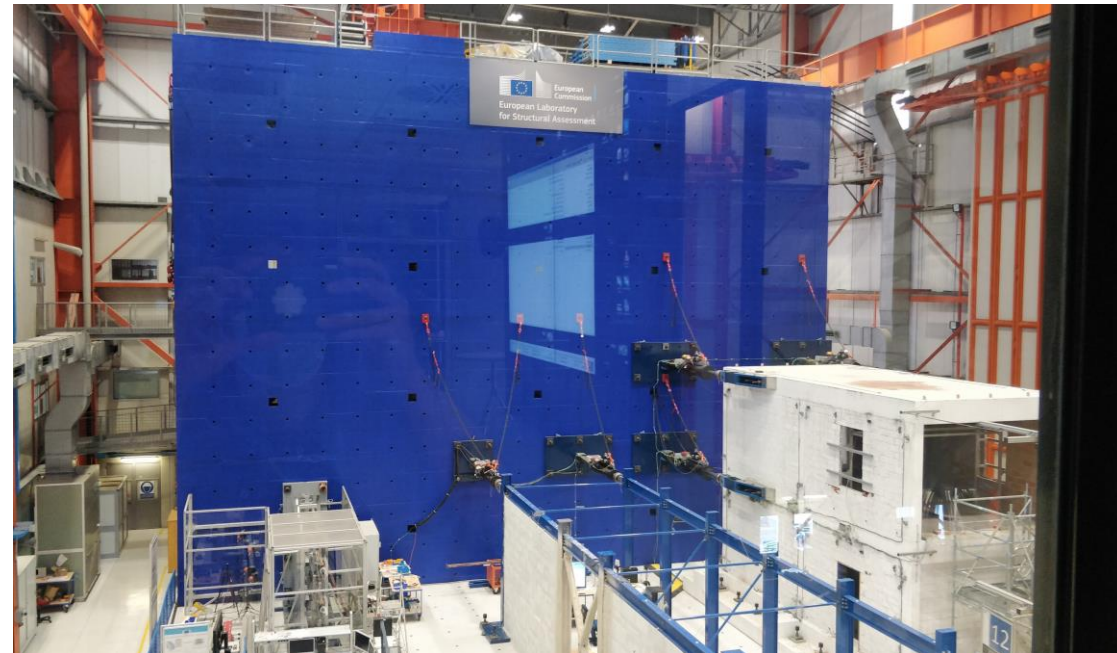


**Are behavioural
biometrics powerful
enough as a standalone
authentication
mechanism?**

Joint Research Centre

Joint Research Centre

- Bridge between science and policy for the European Commission
- 3000 researchers
- 5 sites in Geel, Karlsruhe, Petten, Sevilla, and Ispra
- Former Italian nuclear research site
- ELSA laboratory
- VELA laboratory



Thank you

Andraž Krašovec

andraz.krasovec@ec.europa.eu

Data available at: <https://gitlab.fri.uni-lj.si/lrk/ca-iot>



Univerza v Ljubljani
Fakulteta *za računalništvo*
in informatiko

