WACA: Wearable-Assisted Continuous Authentication Framework with Motion Sensors

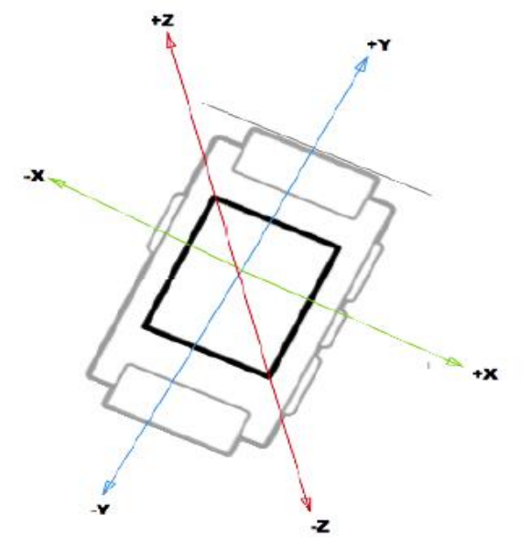
Abbas Acar, Hidayet Aksu, Kemal Akkaya, and A. Selcuk Uluagac
Florida International University
Electrical and Computer Engineering Department
Cyber-Physical Systems Security Lab (CSL)
{aacar001, haksu, kakkaya, suluagac}@fiu.edu

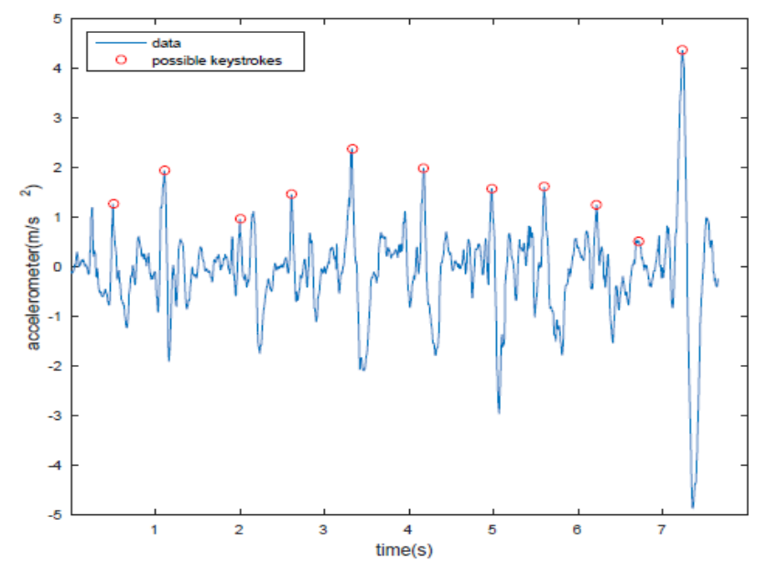
Abstract

Continuous authentication goes beyond the conventional onetime login processes. In continuous authentication, the user is re-verified periodically throughout the login session. However, this is not easily achievable with the existing one-time login systems. Hence, continuous authentication aims to re-verify the user without breaking the continuity of the session. In the meantime, the usage of wearables such as smart watches, fitness bands, heart-rate sensors, etc. in our daily activities is increasing enormously. In fact, the ubiquity of wearable devices can be utilized in continuous authentication settings. In this poster, we present the design of a novel Wearable-Assisted Continuous Authentication (WACA) framework. The framework combines the ubiquitous nature of wearables and usability of continuous authentication. The WACA framework can be applied transparently to an already existing one-factor authentication (e.g., password, token) system. In the WACA framework, the data is acquired through the built-in sensors of a smartwatch. The framework incorporates 15 different sensory features along with distance measure methods and a rich set of machine learning algorithms for the identification and authentication purposes. Furthermore, we evaluate the performance of WACA with real devices and data. Our evaluation demonstrates the functionality and feasibility of the WACA framework. Specifically, our results show on average 16% FAR and 5% FRR for the authentication while the accuracy rates of identification are 100% for MLP algorithms and 89% for Random Forest algorithms.

Wearables and Motion Sensors

- By 2020, there will be 411 million wearable devices with a total of 34 billion global market value [1].
- Wearables have:
  - advance built-in sensors (e.g., accelerometer, GPS, thermometer, heart rate monitoring, etc.)
  - networking capability (e.g., Bluetooth and Wi-Fi)
- Multi-device usage (e.g., laptop, smartphone, tablet, etc.) [2]





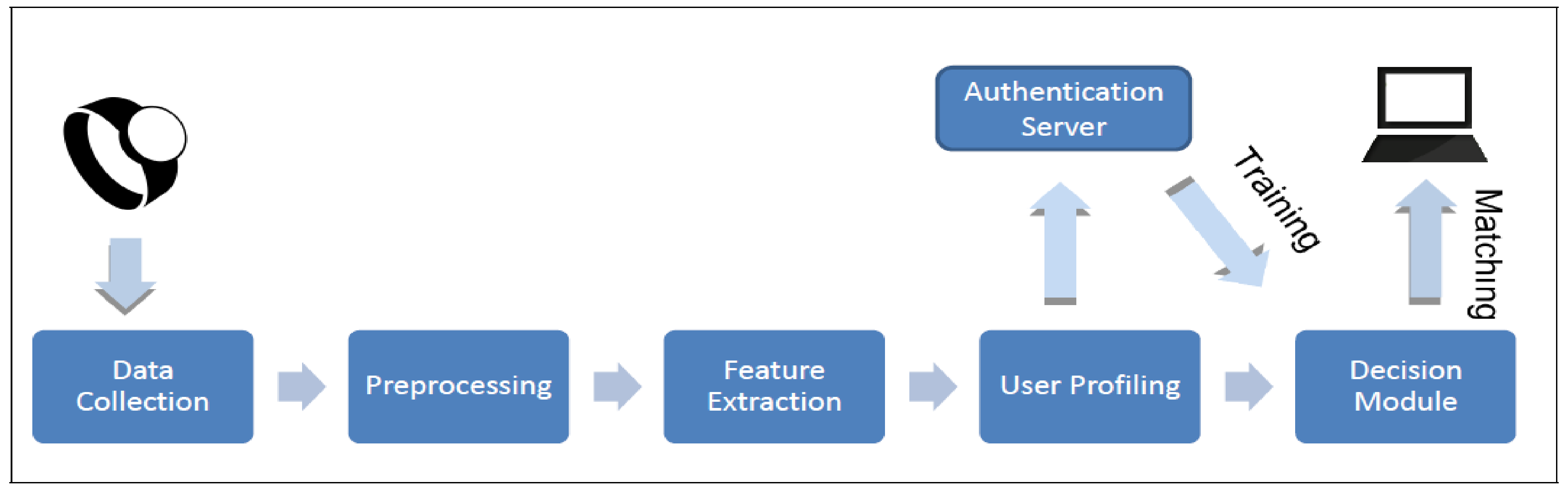
Continuous Authentication (CA)

- Passwords are vulnerable to:
  - Brute-force, dictionary, social engineering, session hijacking, and spyware type of attacks.
- CA methods checks the user's identity during the entire session.
- Continuous (second) factor can be:
  - Behavioral biometrics such as keystroke dynamics, gesture, and gait patterns.
- In our framework, WACA, the second factor is keystroke dynamics.
- Keystroke dynamics can be: *Fixed-text* or *Text-free*

Adversary Model & Assumptions

- Adversary Model:
  1. An attacker or an innocuous friend watching the victim who forgets to lock the computer for a short time to access the victim's computer
  2. An attacker who somehow compromised the first factor (e.g., password, token) of the authentication system
- Assumptions:
  - A user wears a smartwatch with motion sensors and Bluetooth or Wi-Fi while typing
  - Implemented an Android Wear app to collect sensory data
  - Secure Channel is established after pairing

Overall Architecture



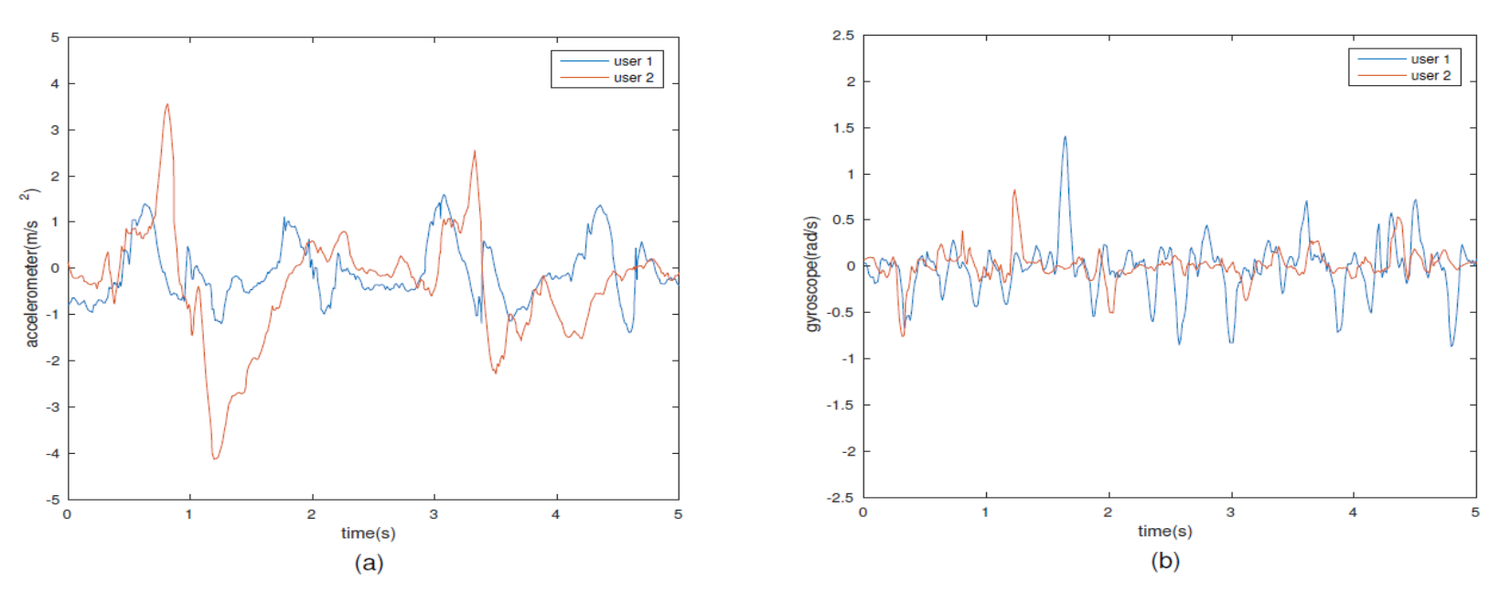
Authentication Server
Training
Matching
Data Collection → Preprocessing → Feature Extraction → User Profiling → Decision Module

- Aim: Combining the ubiquitous nature of wearables and usability of continuous authentication.
- WACA:
  - Is used as a ”second factor”
  - Collects data through smartwatch's motion sensors (i.e., accelerometer and gyroscope)
  - Extracts keystroke dynamics from raw sensor data
  - The feature vector (i.e., user profile) is created to profile the user
  - Decision Module:
    - ✓ Authentication using Distance Measure
    - ✓ Identification using Machine Learning Algorithms

Observations

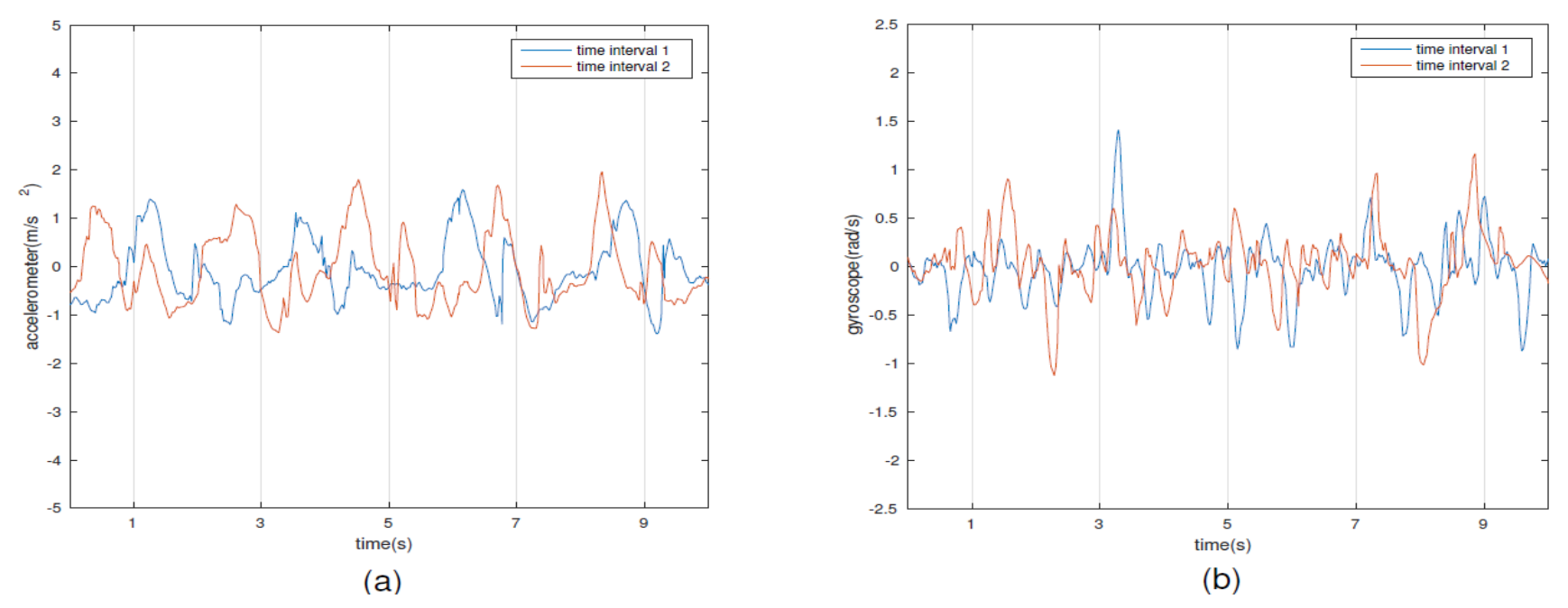
1. First Observation:

- **T**wo different users' sensor data while typing the same text with (a) accelerometer, (b) gyroscope:

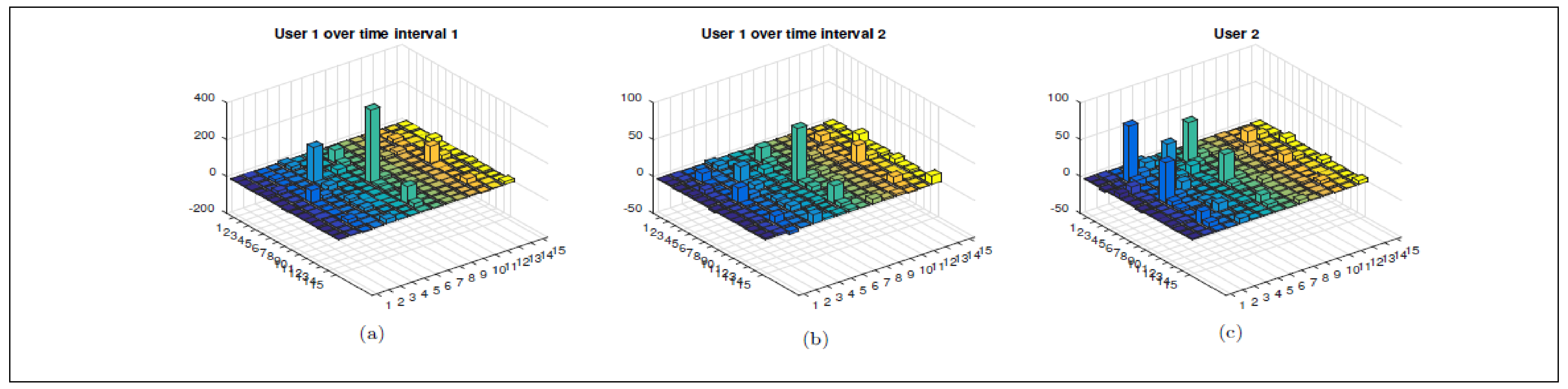


2. Second Observation:

- The same user's sensor data over two different time intervals with (a) accelerometer, (b) gyroscope:



Comparing Different Profiles for Selected Features



- Covariance matrix of three different profiles: (a) and (b) belong to the same user over two different time interval. (c) is the profile of a second user for the same feature set.

Evaluation: Initial Results

- Testbed & Methodology:
  - LG G Watch R
  - Android Wear app:
    - ✓ Registers the sensors
    - ✓ Stores the data to a file in the internal storage
    - ✓ Sampling Rate: *onSensorChanged and SENSOR_DELAY_FASTEST* mode
  - Data is collected via 6-axis motion sensor (3-axis acc + 3-axis gyro)
  - Qwerty keyboard
  - Randomly generated *pangram* sentences
  - 90 features in total (15 features * 6 axis)
  - 4500 samples in total (9 profiles * 500 samples)
- Results:
  - Authentication:
    - ✓ 16% False Acceptance Rate (FAR) and 5% False Rejection Rate (FRR)
  - Identification:

Algorithm	TPR	FPR	Precision	Recall	ROC Area	PRC Area	Accuracy
MLP	1.00	0.00	1.00	1.00	1.00	1.00	100%
Random Forest	0.89	0.06	0.92	0.89	0.95	0.93	89%
kNN	0.78	0.11	0.87	0.78	0.83	0.72	78%
J48	0.89	0.06	0.92	0.89	0.92	0.84	89%

References

1. P. Lamkin. Wearable tech market to be worth $34 billion by 2020 @ONLINE, Feb. 2016, http://www.forbes.com/sites/paullamkin/2016/02/17/wearable-tech-market-to-be-worth-34-billion-by-2020/#f3e57cd3fe38
2. G. Sterling. Study: 60 percent of adults switch screens during the day @ONLINE, Mar. 2014, http://marketingland.com/study-60-percent-adults-switch-screens-day-76130
3. S. Mare, A. M. Markham, C. Cornelius, R. Peterson, and D. Kotz. Zebra: zero-effort bilateral recurring authentication. In *Security and Privacy (SP), 2014 IEEE Symposium on*, pages 705{720. IEEE, 2014

Acknowledgements

This work was partly supported by NSF-CAREER-CNS-1453647.