Weaponizing IoT Sensors: When Table Choice Poses a Security Vulnerability

Gustavo Casqueiro

Military Institute of Engineering, Rio de Janeiro, Brasil

Sayed Erfan Arefin, Tasnia Ashrafi Heya, Abdul Serwadda, Hassan Wasswa

Texas Tech University, Lubbock, Texas, USA

December 15, 2022

Motivation

- We investigate the question:

  -"Whether a series of vibration sensors hidden under the keyboard, or table could be used to infer the text typed on the keyboard?"

- A new paradigm of **attack introduced**

Introduction

- An **attack to snoop PINs typed on the keyboard**
- Underside of keyboard is **rigged with small motion sensors (i.e., 1.5cm)**
- Investigation of attack behavior for **sensors hidden under tables**
  - four commonly used table-top surfaces
- Investigation of impact of **table rotation and translation on attack behavior**

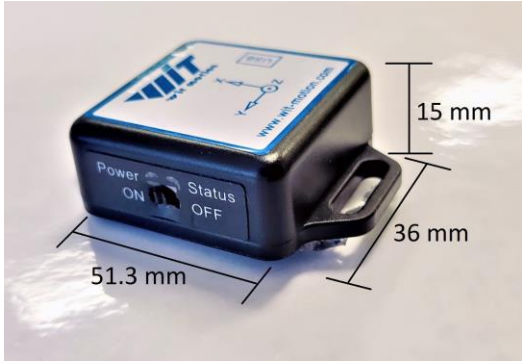


Fig 1: Motion sensor

Threat Scenario

- **Two variants of the attack:**

  - with sensors, i) under keyboard and ii) under table (Fig 2)

- Attack would typically be executed by
  - spying on victim's keyboard inputs
  - an insider with frequent access to victim's computer

    - colleagues, office cleaners, roommates, employers, etc.

- For training data, the attacker has 2 options:
  - replicate the victim's setup
  - use the victim's very system for typing

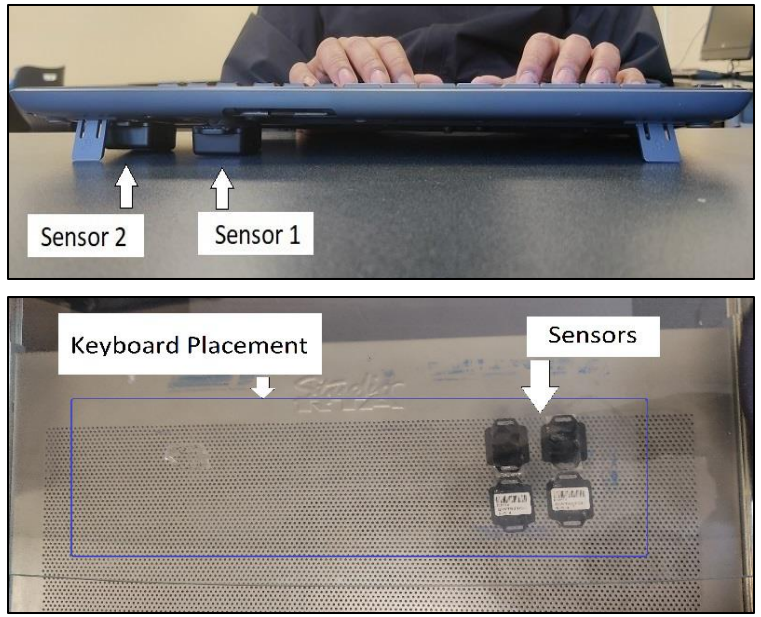
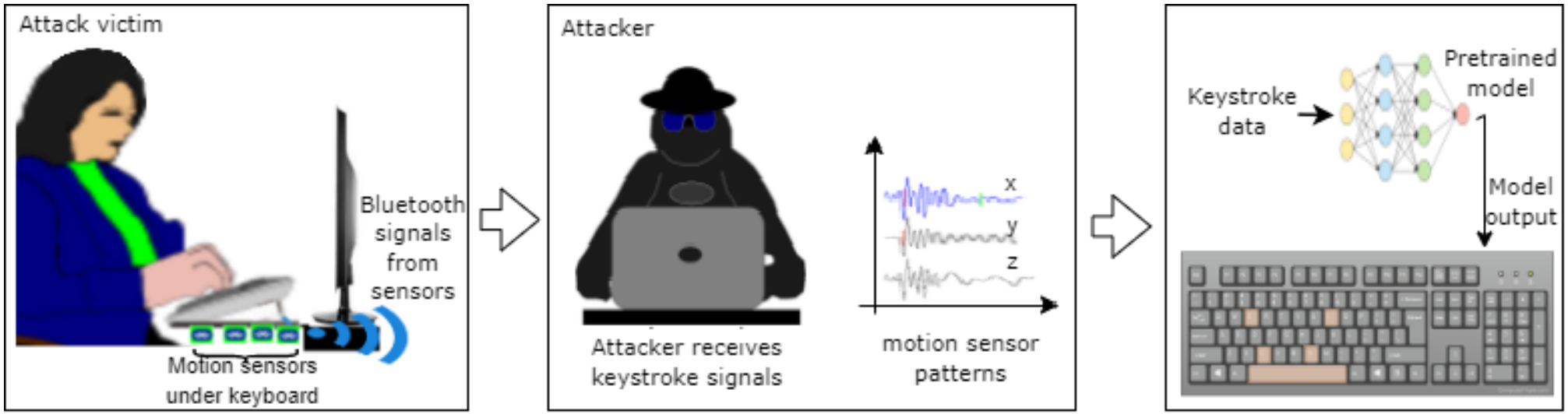


Fig 2: Sensor placement under the keyboard and glass table .

Attack Design



Attack victim typing on a keyboard with a bluetooth enabled motion sensor planted under it

Attacker running sensor software activates bluetooth signal receiver and extracts keystroke data from captured motion sensor signals

Model predicts sequences of pressed keys from keystroke data as highlighted on the keyboard

Fig 3: Overview of our attack.

Data Collection I

- Sensors used: Witmotion's WT901BLECL model
  - stealthily attach under table or raised end of a keyboard (Fig 2)
  - has 3-axis accelerometer, gyroscope, angles and magnetic fields
  - **transfers data** to Android or Windows devices **via Bluetooth**

- Sensors placed under the numeric pad

Data Collection II

- Data collection involved 23 participants for all Experiments
- For training data:
  - typed 0 to 9, each 3 times
- For testing data:
  - mixed pins of 4, 6 and 8 digits length
  - typed 5 PINs of each length (total 15)

Four Different Table Representation

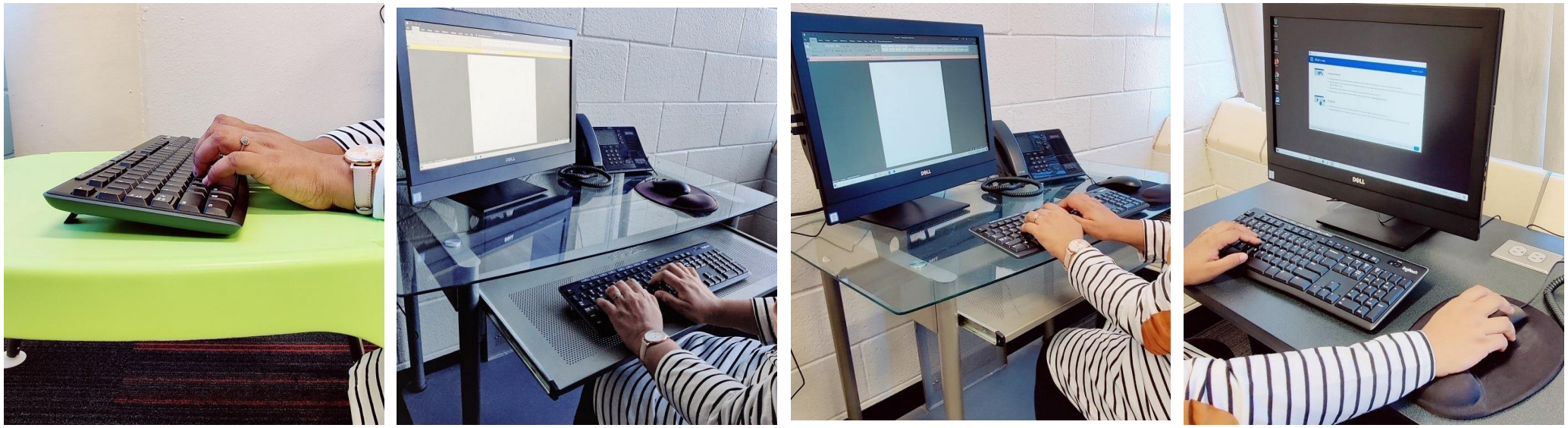


Fig. 4: Data collection on tables of four different table materials under which sensors have been attached.

Data Processing and Feature Extraction

- Attack is centered on identifying pauses and wrist motions following three steps:
  i. initiate attack by holding hand still for ($t_1 \pm \varepsilon$) seconds (as **opening pause**)
  ii. writing letter “A” (or mimic writing “A”) and
  iii. another pause of ($t_2 \pm \varepsilon$) seconds (as **closing pause**)
- g_x is flagged as part of pause if $-T_h \leq g_x \leq T_h$

Evaluation

- Keystroke Inference Attack
- Detecting Keyboard Movements

Keystroke Inference Attack

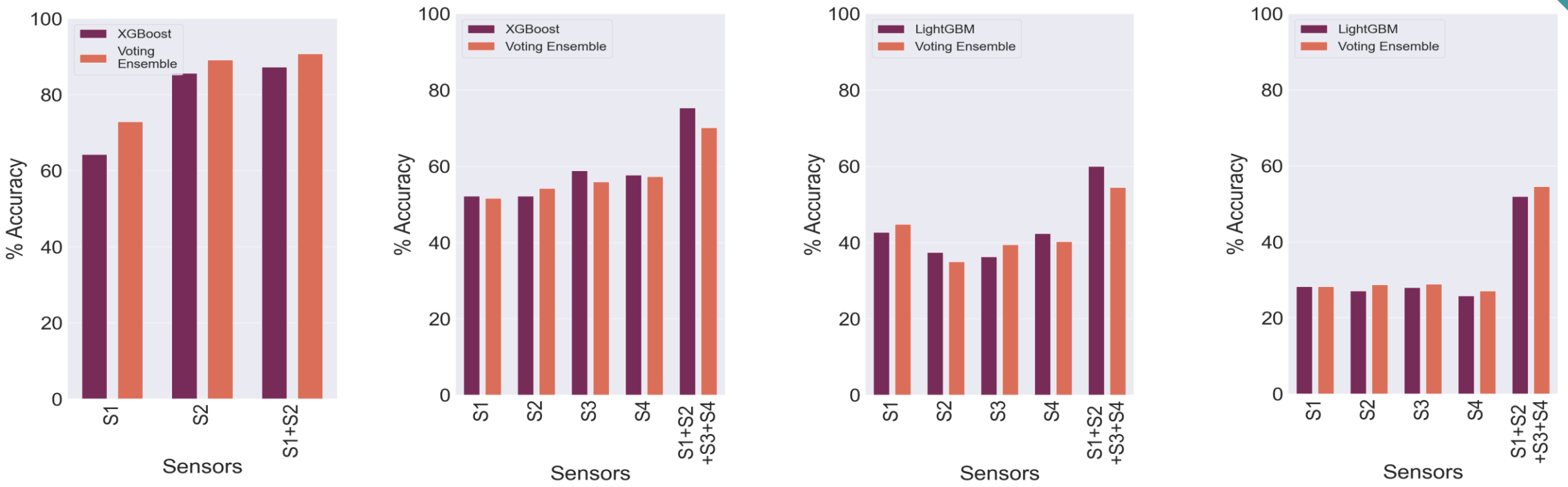
- 10-class problem involving the numbers 0-9
- Different Surfaces
  i. 2 sensors placed directly under the keyboard.
  ii. Keyboard placed on a **Plastic table** and 4 sensors placed under the table
  iii. Keyboard placed on a **Glass table** and 4 sensors placed under the table
  iv. Keyboard placed on a **Metallic table** and 4 sensors placed under the table

Keystroke Inference Attack

- Classifiers used
  i. XGBoost
  ii. Light GBM
  iii. Voting Ensemble

Classification Results

Fig 5: Keystroke inference performance on the 10-class problem involving the numbers 0-9.



- Sensors under keyboard
- Sensors under Plastic table
- Sensors under glass table
- Sensors under metal table

Classification Results II

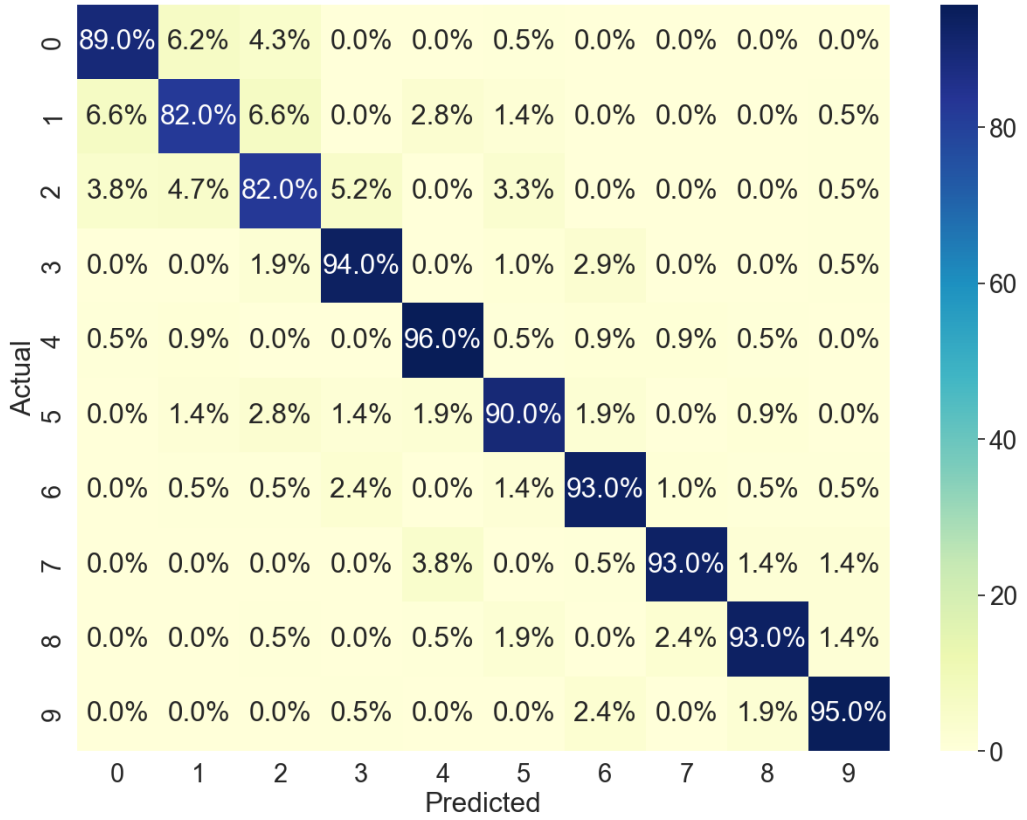


Fig 6: Confusion Matrix for the Voting Ensemble when the sensor was under the keyboard

Accuracy-Distance Relation

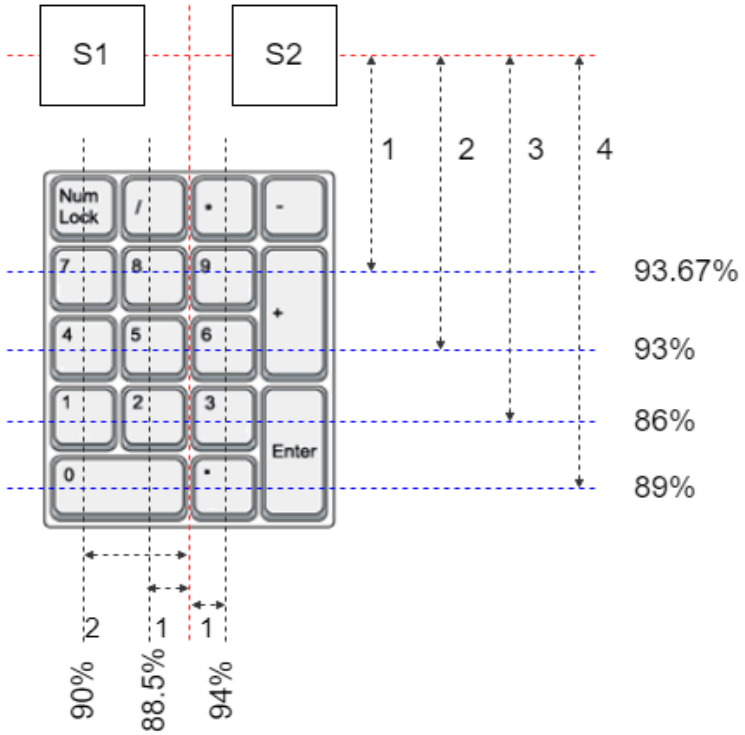
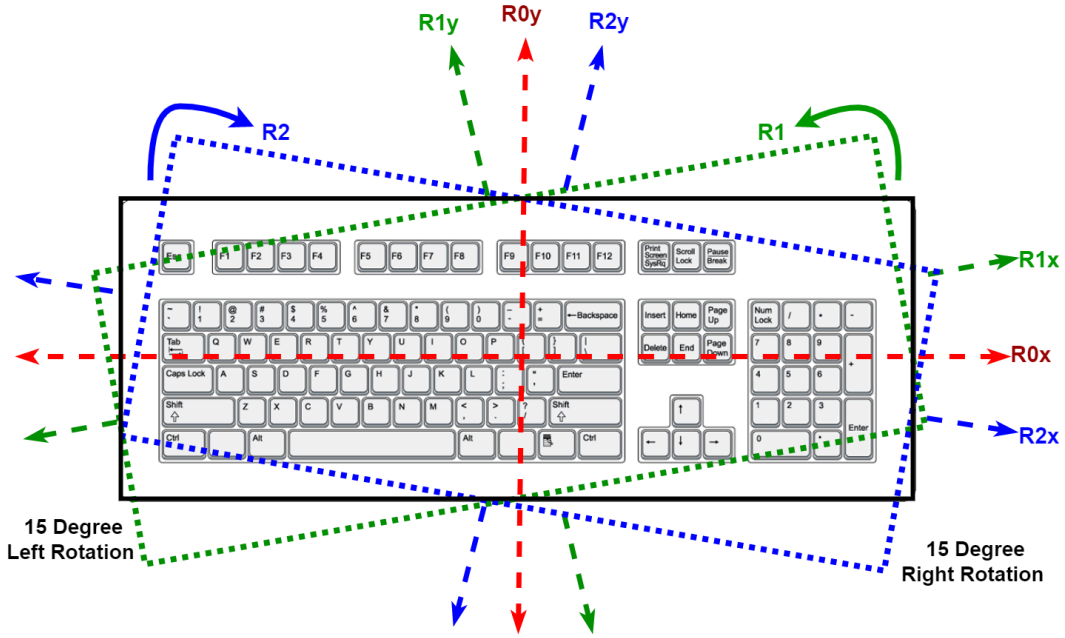


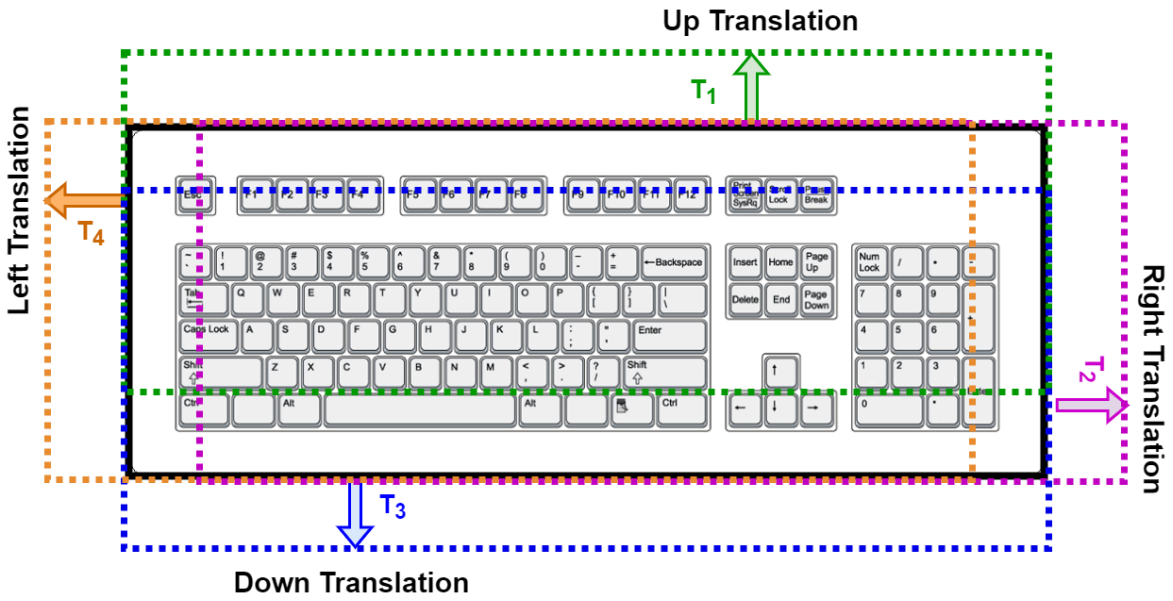
Fig 7: Accuracy-Distance relation for the Voting Ensemble when the sensor was under the keyboard.

Detecting Keyboard Movements

- Keyboard Rotation

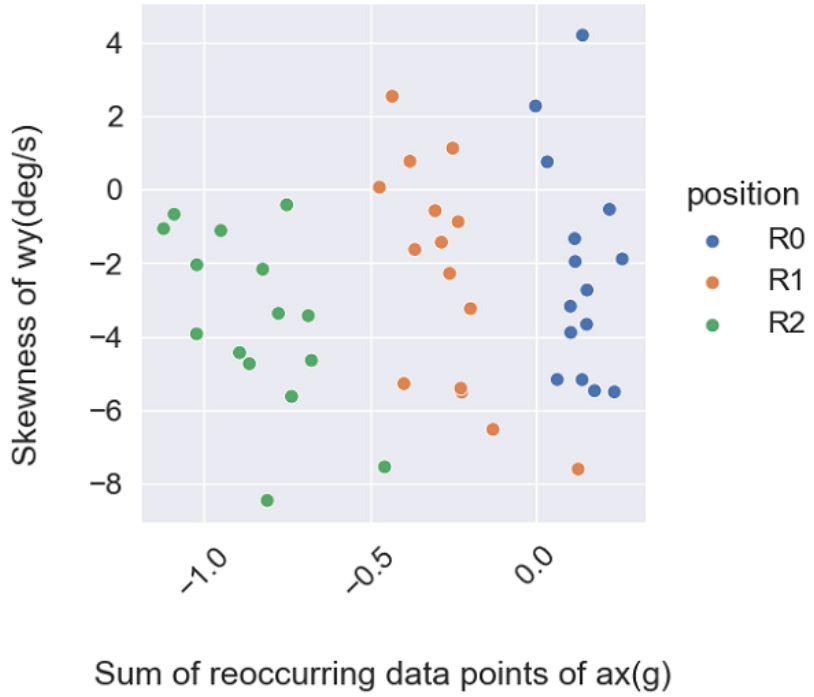


- Keyboard Translation

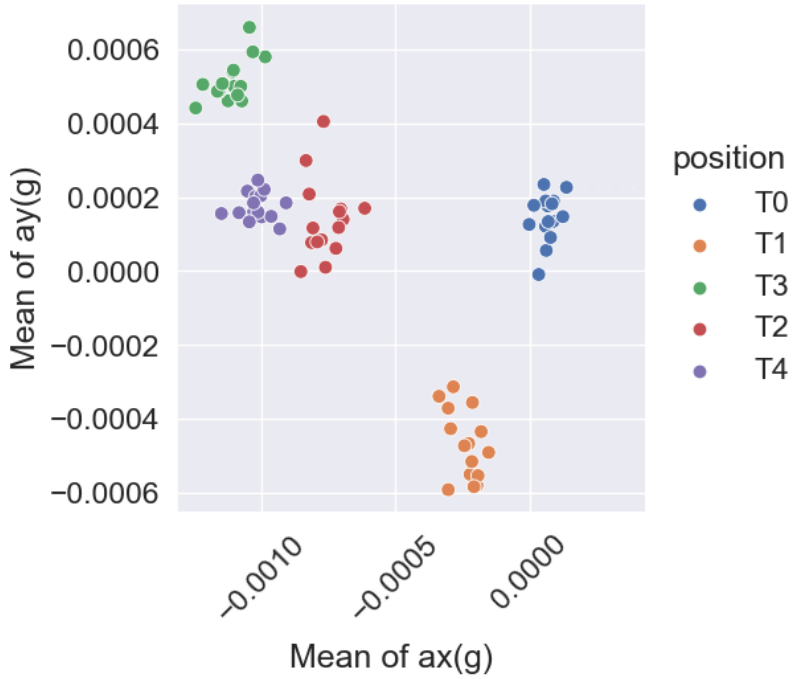


Detecting Keyboard Movements II

- Keyboard Rotation



- Keyboard Translation



Thank You