SaTC: TTP: Small: Collaborative: Privacy-Aware Wearable-Assisted Continuous Authentication Framework
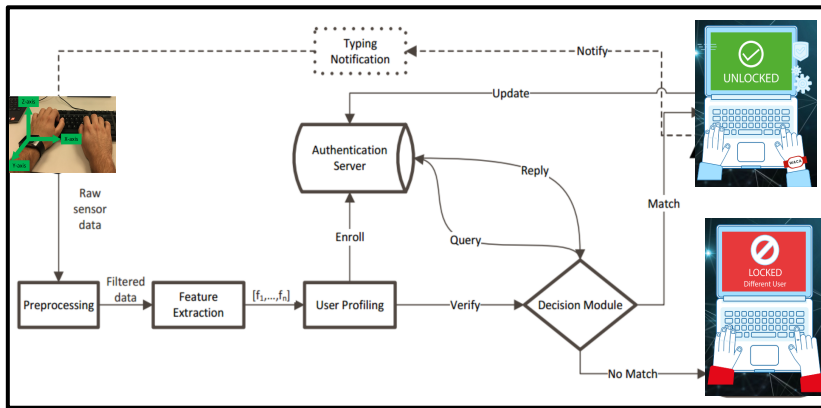
Challenges

Authentication

Passwords are subject to:
- Social engineering attacks
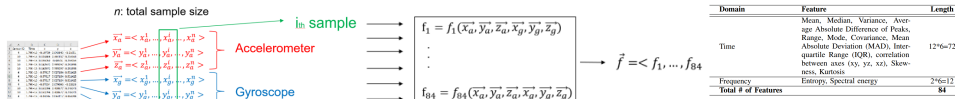- Session hijacking
- Insider attacks
- Compromised database

Privacy

- Biometrics raises privacy concerns.
- No need to share the template with third parties
- Secure template matching techniques can address this issue

Technical Approach
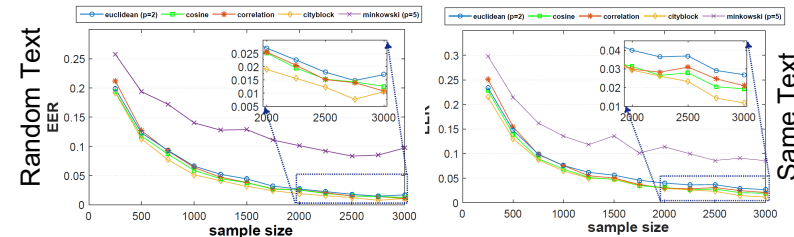

- Wearable-assisted Continuous Authentication
  * Aim: Using the ubiquitous nature of wearables for the usability of continuous authentication.
  * Key observation: Each person's wrist movements & actions are completely unique while typing.
- Privacy-aware Authentication through NTTSec

Performance

- Authentication results
  - 30 seconds of the data → 0.01 error rate
  - 20 seconds of the data → 0.02 error rate
- Identification results
  a. Same text: 5 samples and 1500 samples size → 99.2% accuracy
  b. Random text: 5 samples and 1500 samples size → 99.2% accuracy

Scientific Impact

- Combining the use of IoT and biometrics for continuous authentication
- Investigation of privacy-aware applications in the settings of continuous authentication

Broader Impact:

- Broder use of continuous authentication
- Increasing the use of IoT for greater efficiencies
- Applying our privacy-aware methods to other similar authentication systems