Continuous Authentication using Multimodal Behavioural Biometrics

Soumik Mondal

Gjøvik University College, Gjøvik, Norway

Continuous Authentication

- What is that ?
- Why we need this ?

How we can implement this?

- Password based
  - Periodic
  - Annoying
- Biological Biometrics
  - Special Hardware is required
  - Computation Complexity is very high
- Behavioural Biometrics

Why Behavioural Biometrics???

- No special Hardware is required
- Unobtrusive
- Less computational power is required

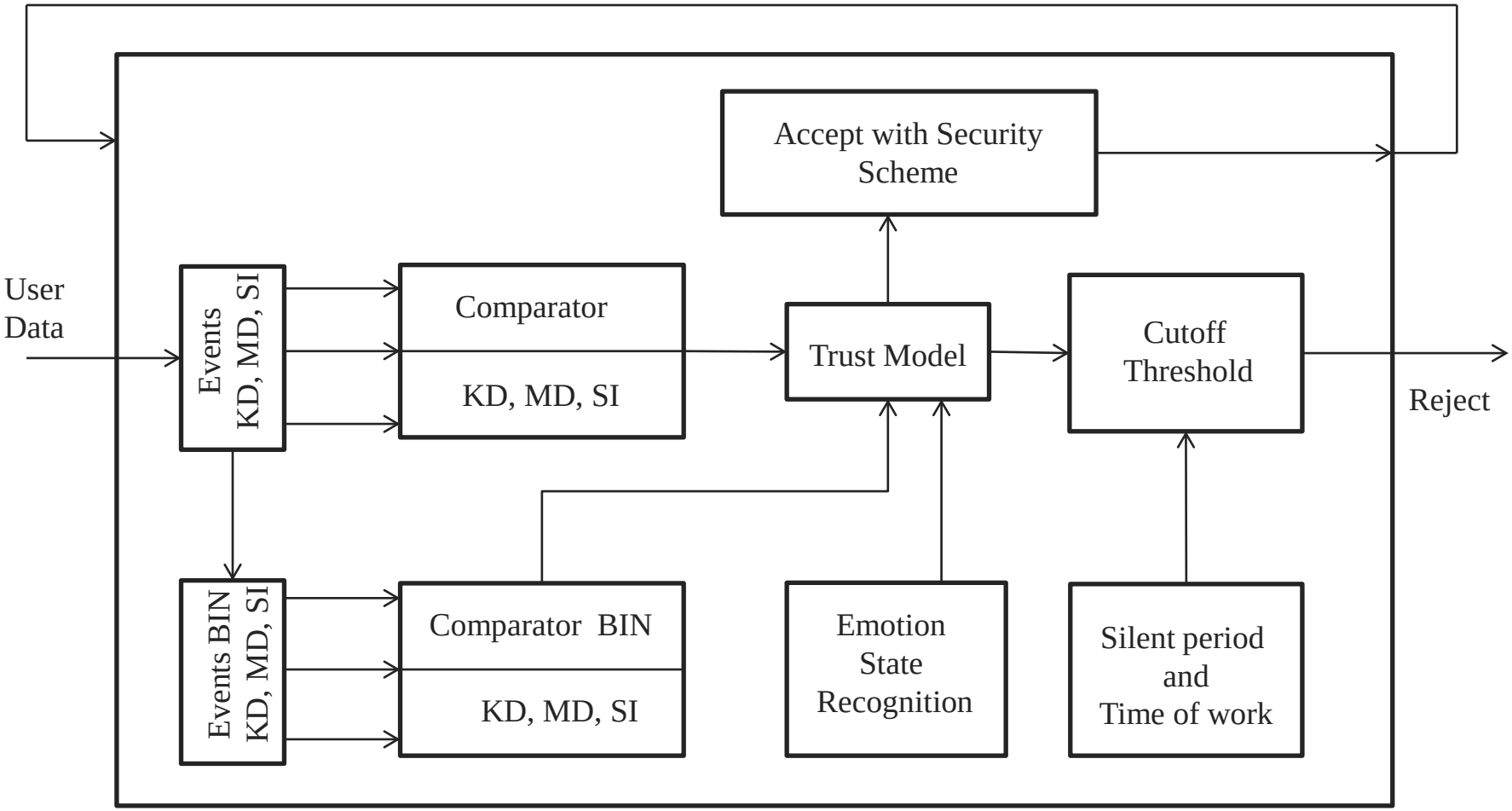
Behavioural Biometrics

- Keystroke Dynamics
- Mouse Dynamics
- Software Interaction

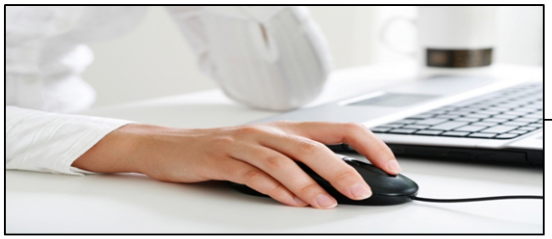
Why these three???

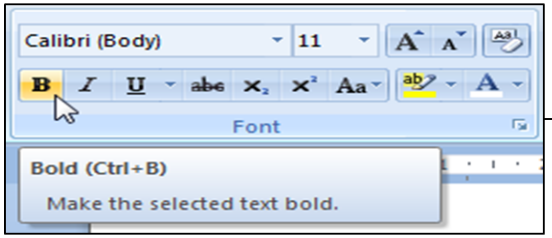
- Increase the performance
- Create a reference for each input device

Architecture of the System



Multimodal





Comparator

KD Template

Comparator

MD Template

Comparator

SI Template

To upper layer

User Template

- Multiple template for the same user
  - Emotion State
  - Time of work

Trust Model

- Start with 100 (%) trust
- Increase or Decrease according to the distance value (d).
- System lockout below threshold (if C<Tr)

$$C := \begin{cases} 100 & Start\ Value \\ Max(C-1,0) & d \leq T \\ Min(C+1,100) & d > T \end{cases}$$

Result on continuous keystroke dynamics dataset

- Applied on continuous keystroke dynamics dataset [1]
- Imposter user was detected on an average after 181 keystroke events with person based Threshold.

1. Bours, P.; , "**Continuous keystroke dynamics: A different perspective towards biometric evaluation**," Information Security Technical Report, Vol. 17, Issues 1–2, pp. 36-43, February 2012.

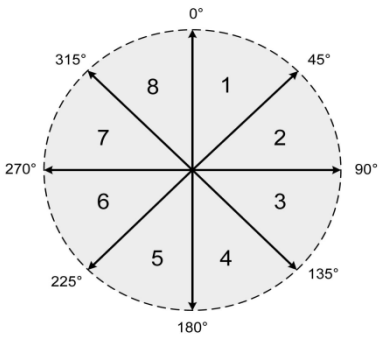
Modified Trust Model

- Start with 100 (%) trust
- Increase or Decrease the trust by classifier score (P).
- System lockout below threshold (if C<Tr)

$$C:=\begin{cases} Min(C+P,\ 100) & P \geq 0.5 \\ Max(\{C-(1-P)\},0) & 0.3 \leq P < 0.5 \\ Max(C-1,0) & P < 0.3 \end{cases}$$

Continuous Mouse dynamics dataset

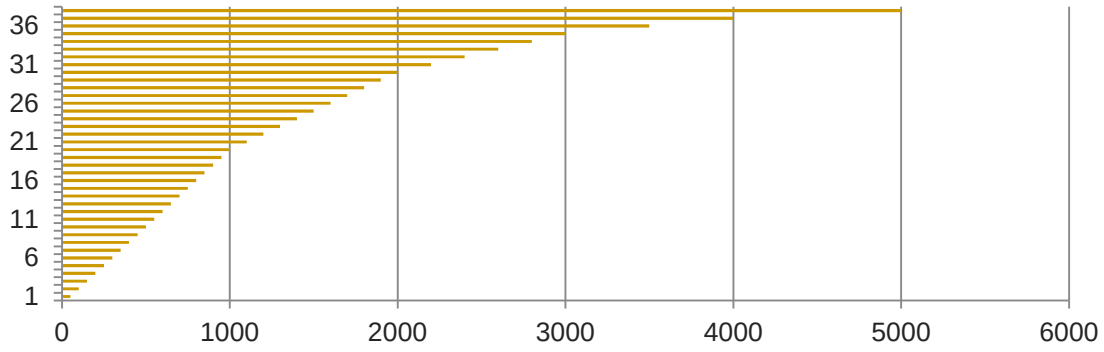
- Applied on continuous Mouse dynamics dataset [2]
- Data Description:
  - Type of Action (1: Mouse Move 2: Silence 3: Point Click 4: Drag drop)
  - Travelled Distance in pixels.
  - Elapsed Time (in seconds)
  - Direction of Movement (1 to 8) (actions performed within 45-degree intervals clockwise).



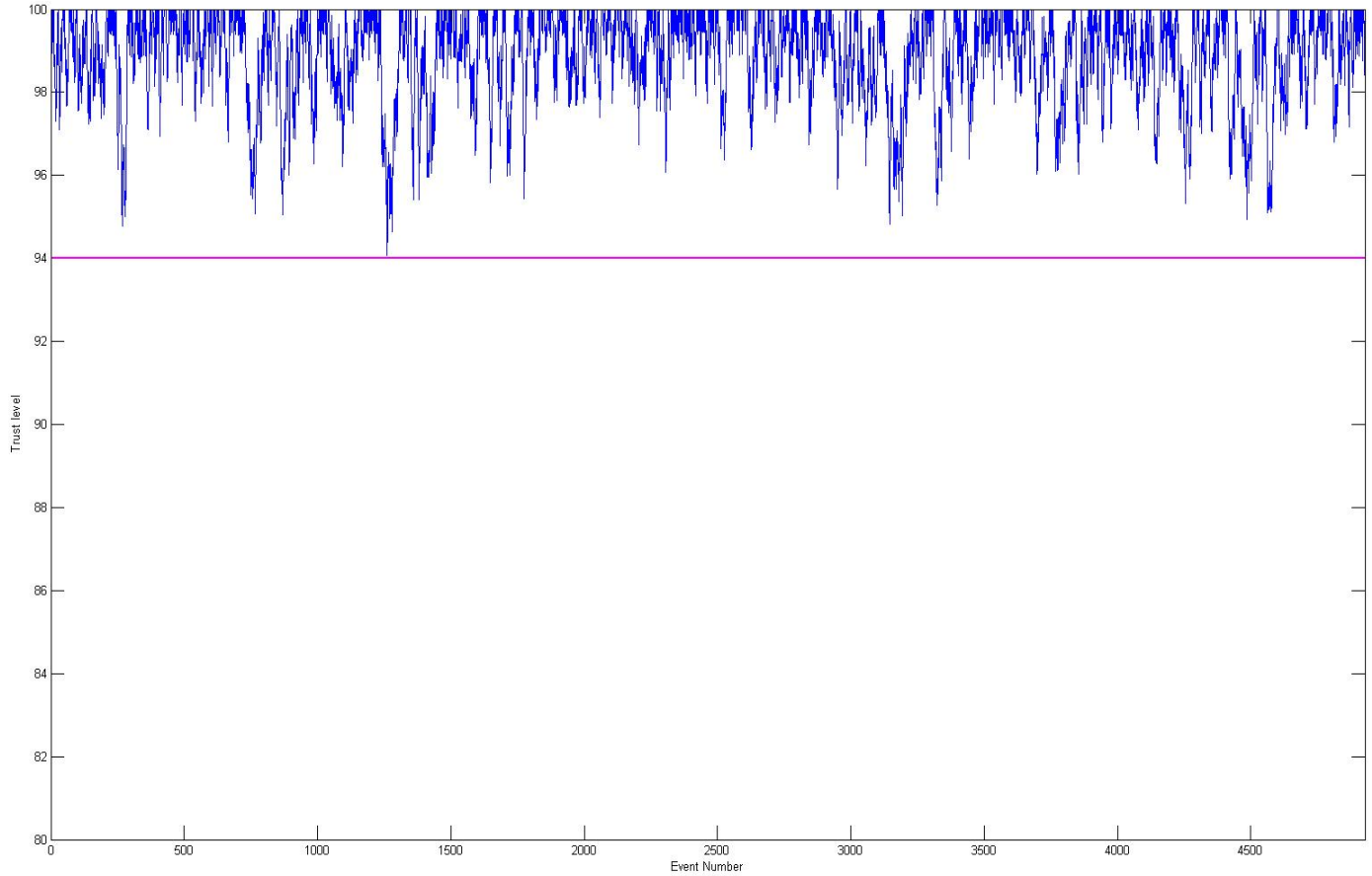
2. Ahmed A.A.E, and I. Traore "**A New Biometrics Technology based on Mouse Dynamics**", IEEE Transactions on Dependable and Secure Computing, Vol. 4 No. 3, July-September 2007, pp. 165-179.

Feature Extraction

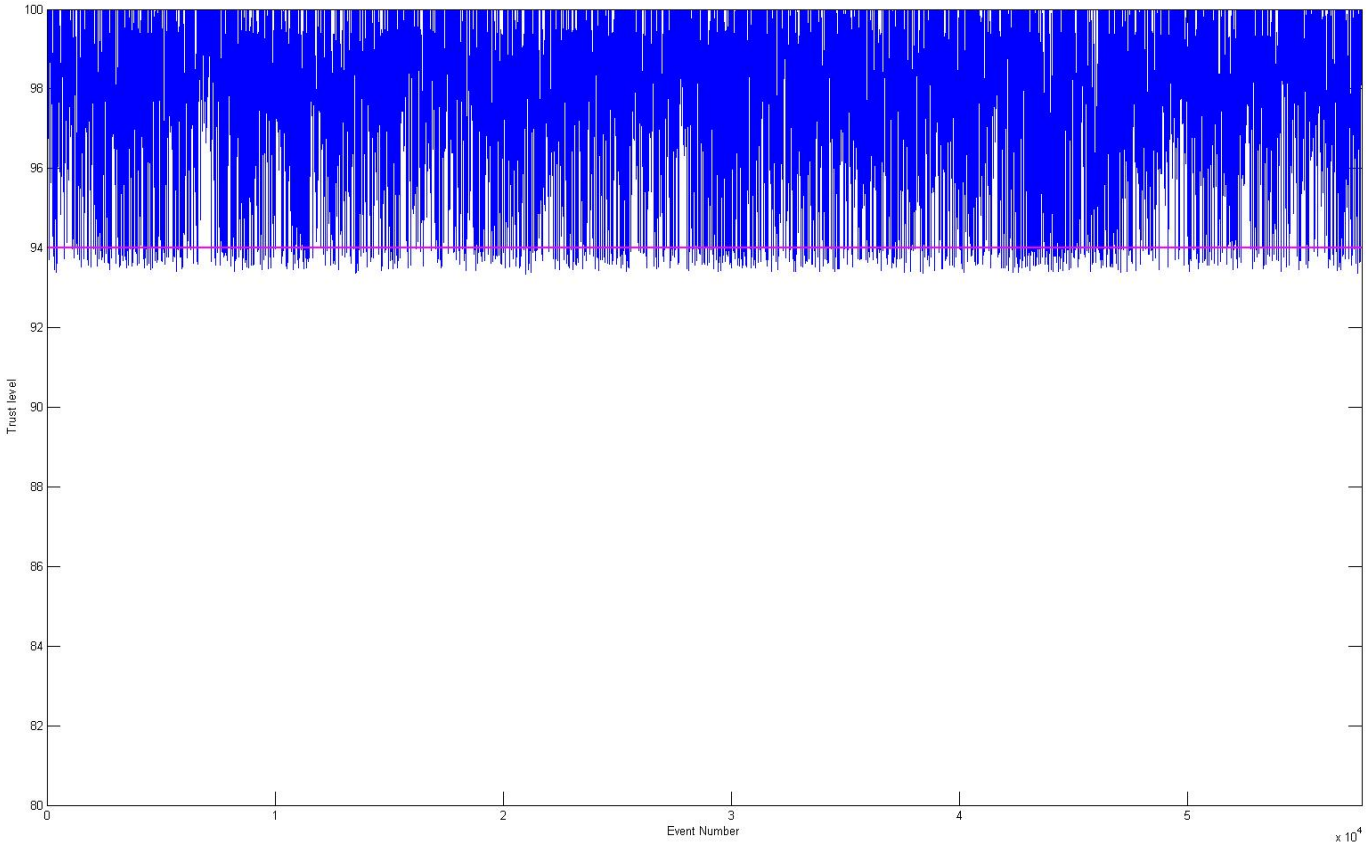
- Type of Action (1: Mouse Move 3: Point Click 4: Drag drop).
- Direction of Movement (1 to 8) (actions performed within 45-degree intervals clockwise).
- Speed of the mouse movement (Travelled Distance in pixels / Elapsed Time).
- Inverse Acceleration of the mouse movement. (Elapsed Time/ Speed)
- Travelled distance in Bins. Total 38 distance bins.



Trust level for Genuine user



Trust level for Imposter user



Result

- Used 41 genuine user and 48 imposter user
- We have used person based threshold
- Genuine user was never detected
- Imposter user was detected on an average after 96 events

Data Collection

- Keystroke Data
- Mouse Data
- Software interaction Data

Data Collection Software

- BeLT Demo

Thank You