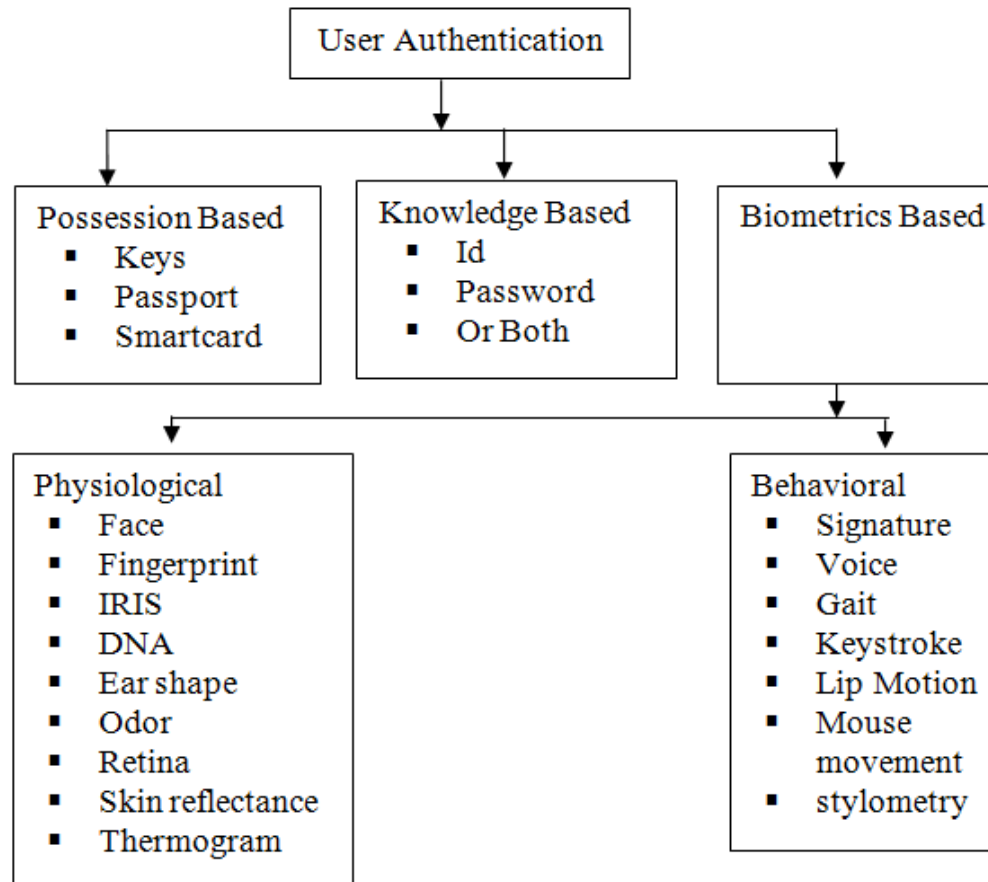# Authentication and Identification Methods Used in Keystroke Biometric Systems

Md Liakat Ali, Charles C. Tappert,
Meikang Qiu, and **John V. Monaco**

Seidenberg School of Computer Science and Information Systems
Pace University, Pleasantville, NY 10570, USA
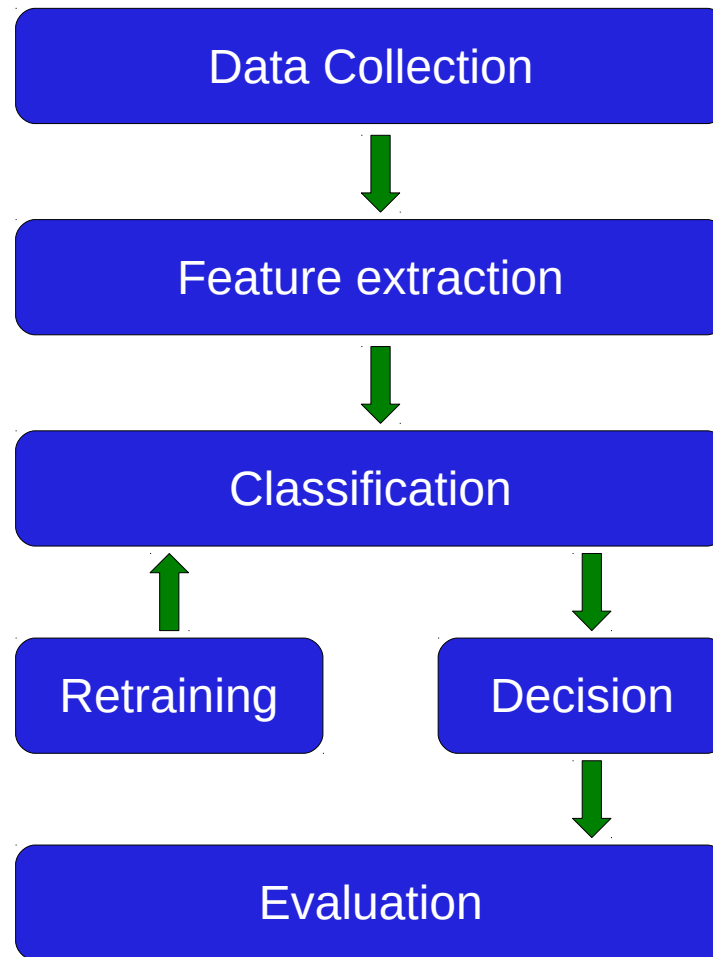
Authentication methods

User Authentication

Possession Based
- Keys
- Passport
- Smartcard

Knowledge Based
- Id
- Password
- Or Both

Biometrics Based

Physiological
- Face
- Fingerprint
- IRIS
- DNA
- Ear shape
- Odor
- Retina
- Skin reflectance
- Thermogram

Behavioral
- Signature
- Voice
- Gait
- Keystroke
- Lip Motion
- Mouse movement
- stylometry

Newell's time scale

Scale (sec)	Time Units	System	World (theory)
10^7	Months		**SOCIAL BAND**
10^6	Weeks		
10^5	Days		
10^4	Hours	Task	**RATIONAL BAND**
10^3	10 min	Task	
10^2	Minutes	Task	
10^1	10 sec	Unit task	**COGNITIVE BAND**
10^0	1 sec	Operations	
10^{-1}	100 ms	Deliberate act	
10^{-2}	10 ms	Neural circuit	**BIOLOGICAL BAND**
10^{-3}	1 ms	Neuron	
10^{-4}	100 μs	Organelle	

Keystroke →

Keystroke biometric system

BigDataSecurity 2015

Types of input

Long free-text

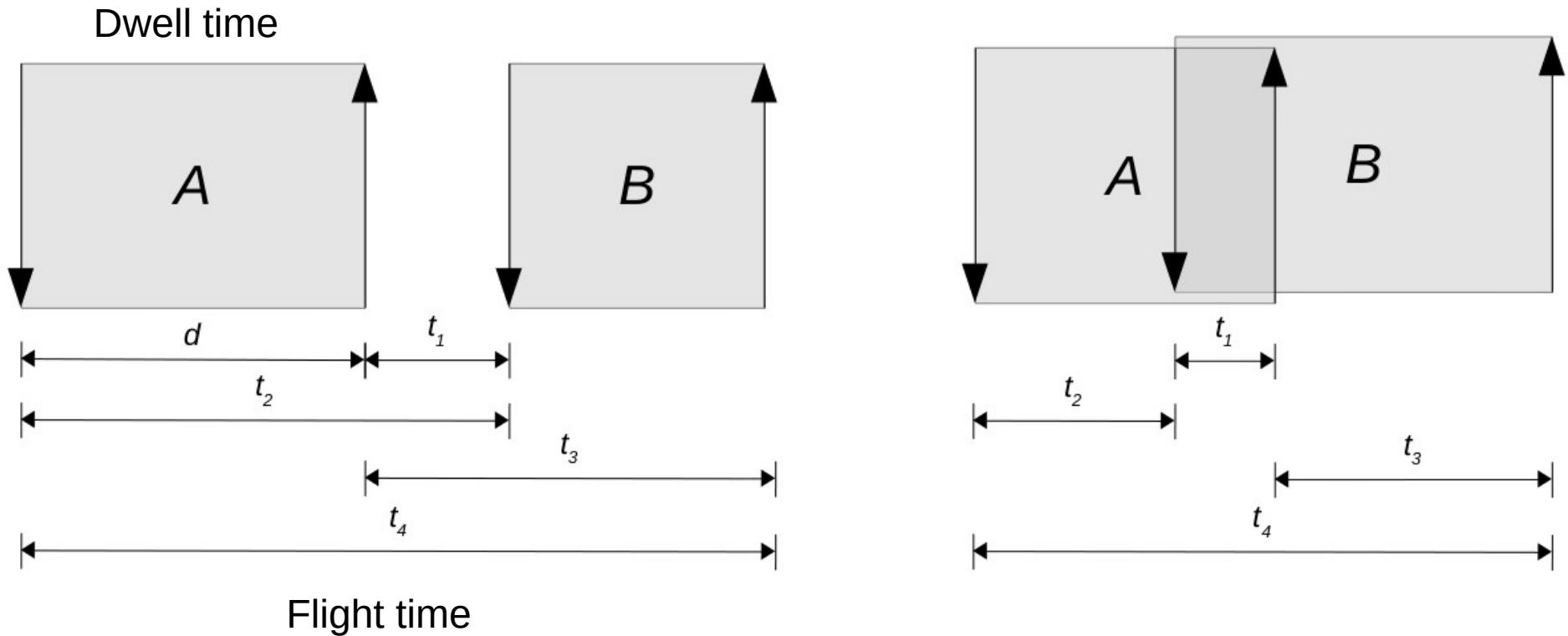Lorem ipsum dolor sit amet,
consectetur adipiscing elit, sed do
...

Long free-text

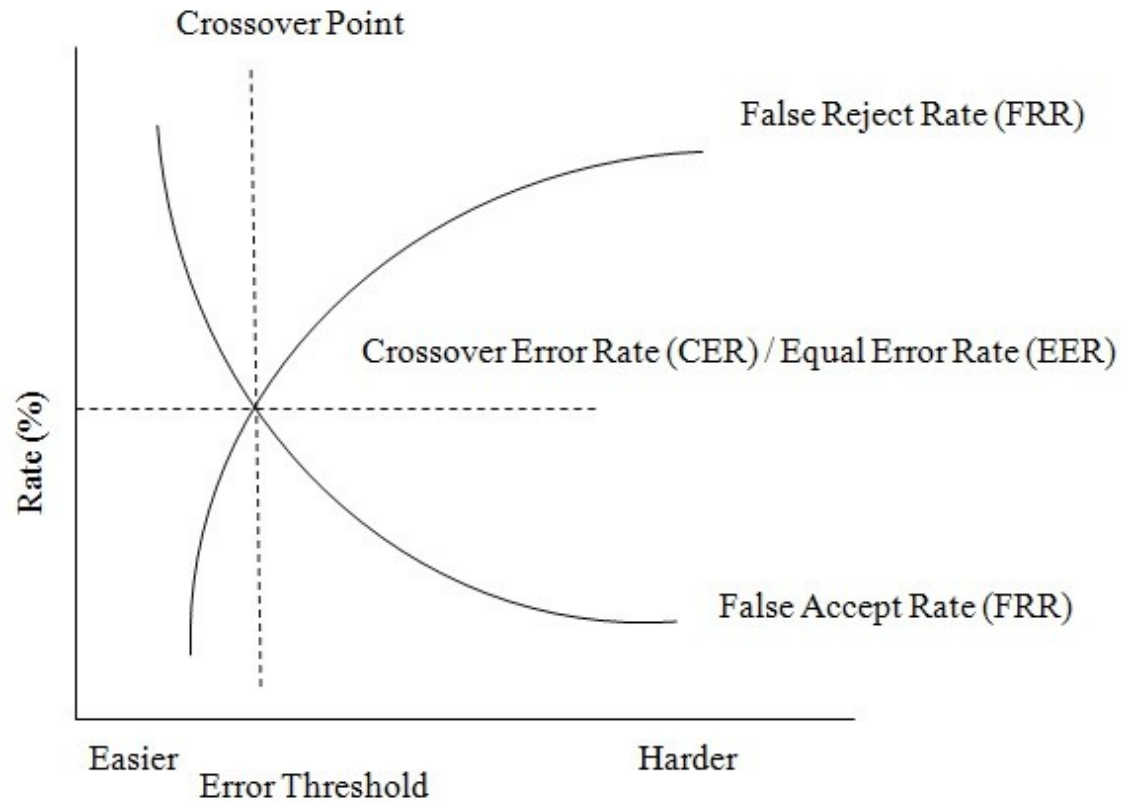Mary had a little lamb,
His fleece was white as snow.

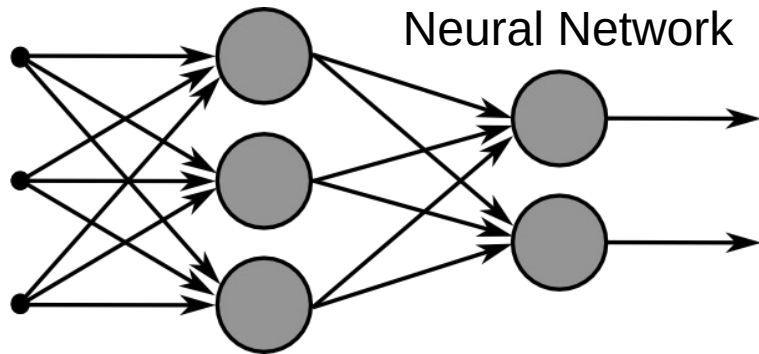**Short fixed-text**

914 555 1234

Keystroke timings

Dwell time

Flight time

Authentication performance

BigDataSecurity 2015

Discriminative methods

Neural Network

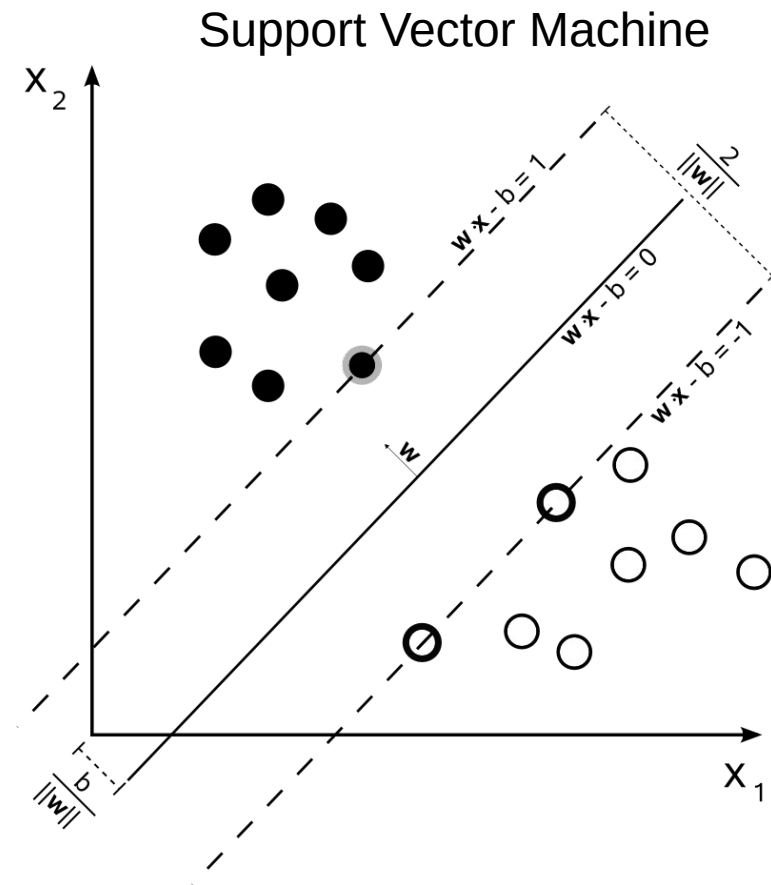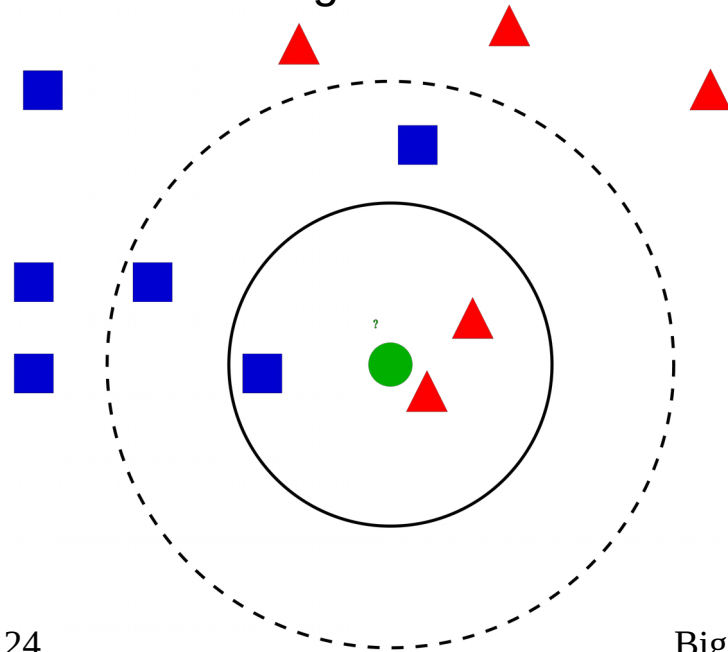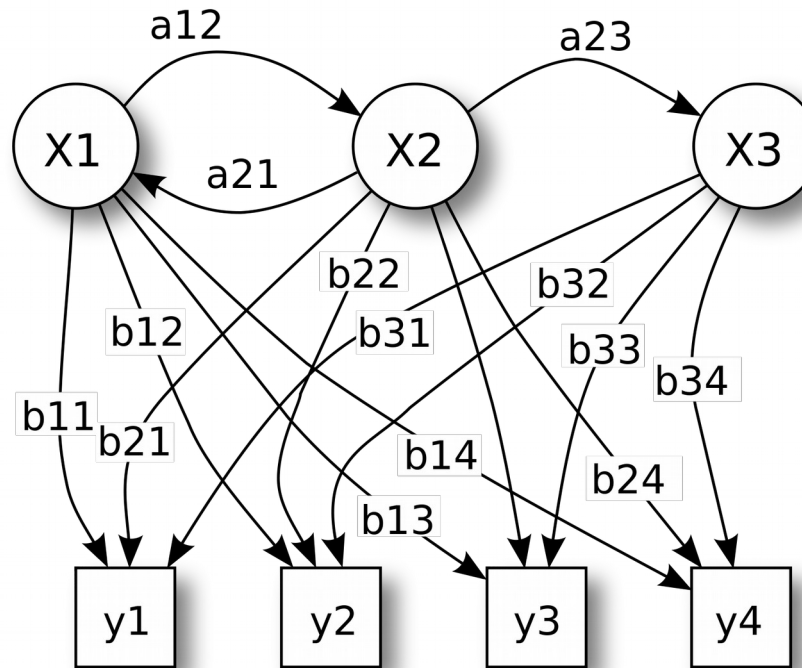Support Vector Machine

K-Nearest Neighbors

Generative methods

Hidden Markov Model

Overall performance

- Long free text: **< 10% EER**

- Short fixed-text: **10-20% EER**

- Depends on:
  - Number of enrolled users
  - Size and quality of training data
  - Keyboard type

Future research

- Representative populations
- Feature engineering
- Real-time systems
- Template aging
- Benchmark datasets

Thank you