Sequential Keystroke Behavioral Biometrics for Mobile User Identification via Multi-view Deep Learning

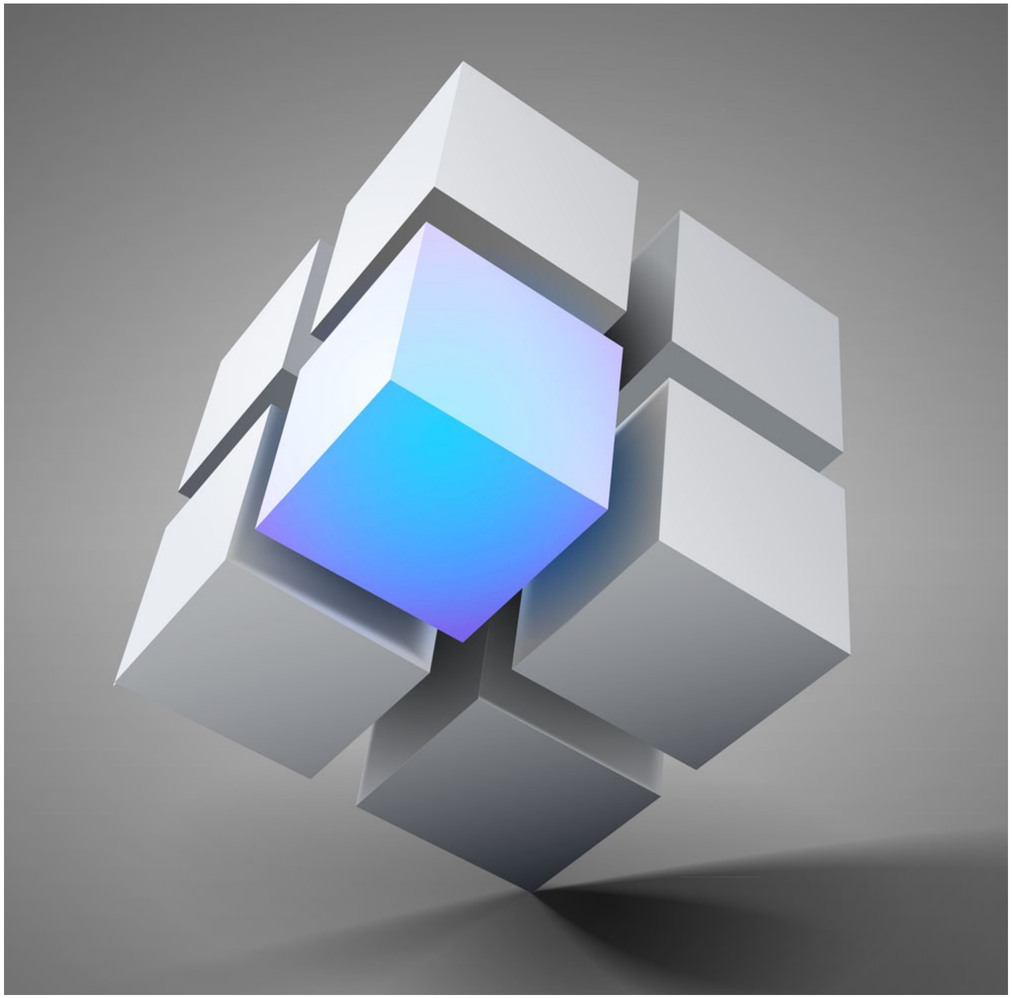
Lichao Sun[1], Yuqi Wang[2], Bokai Cao[1], Philip S. Yu[1,3], Witawas Srisa-an[4], and Alex D Leow[1]

[1]University of Illinois at Chicago, [2]Hong Kong Polytechnic University, [3]Tsinghua University, [4]University of Nebraska Lincoln

Presenter: Jundong Li

E-mail: jundong.li@asu.edu

OUTLINE



1 **Problem**

2 Methodology

3 Experiments

4 Conclusions

Problem Statement

Backgrounds

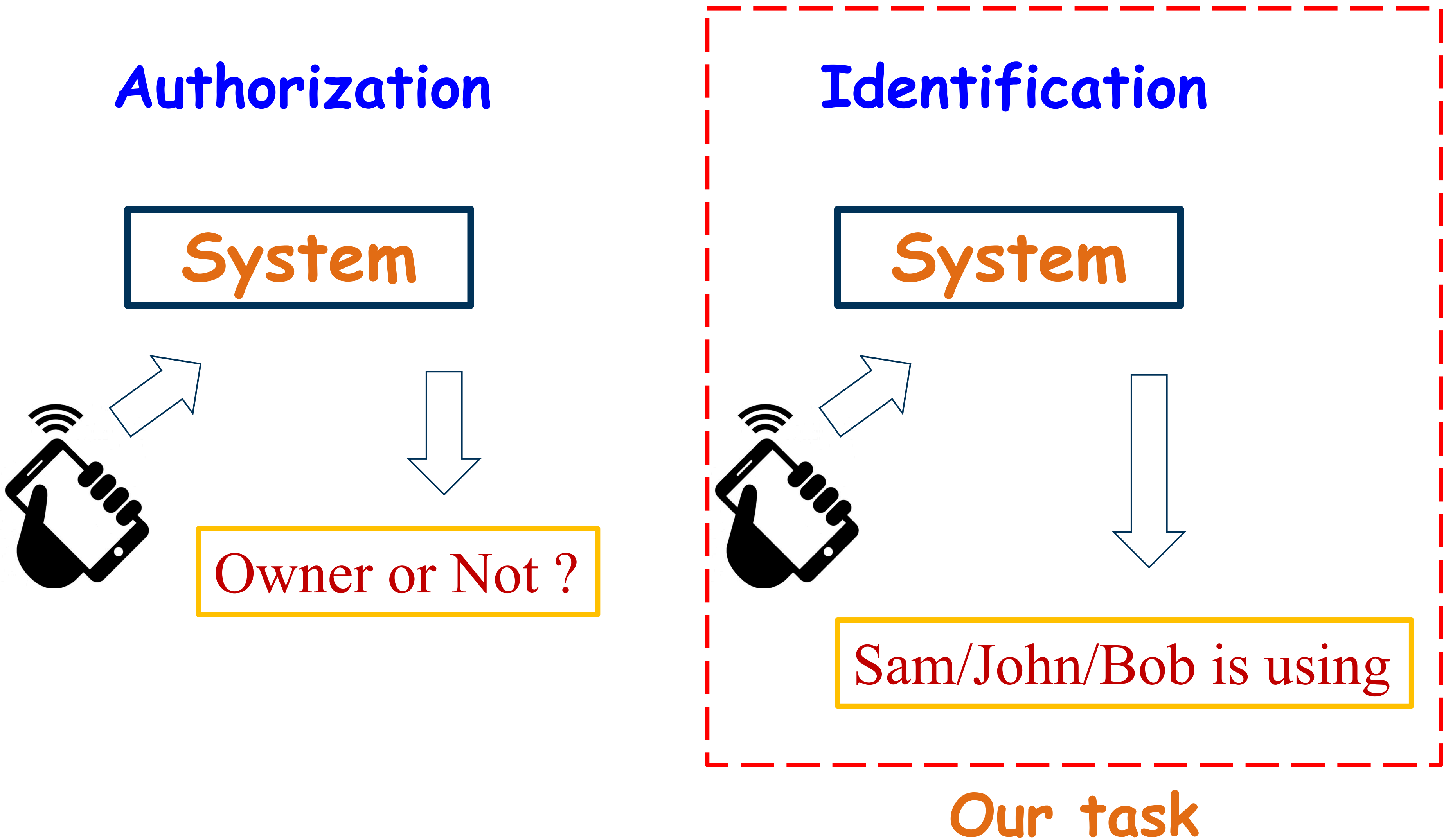
Our task

Who?

What?

Why?

Problem Statement



Problem Statement

Authorization	vs	Identification
• Stolen Phone		• Recommendation
• Using the Phone without Owner's Permission		• Auto Personal Setting Changing

Problem Statement

Traditional Identification

Account

+

Passward

Weakness:

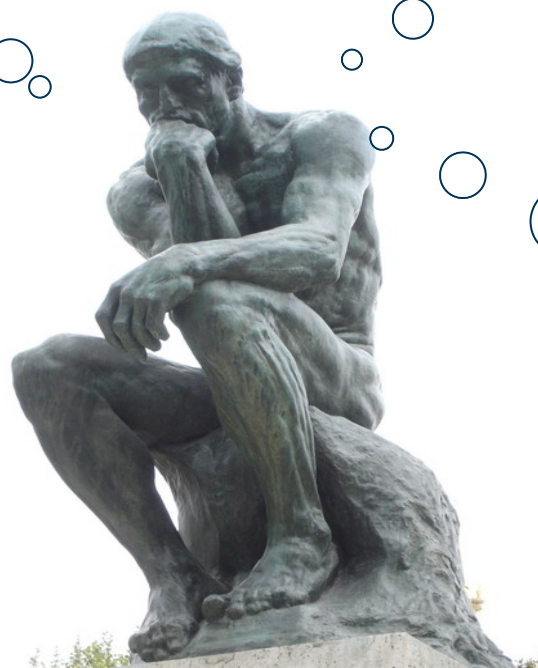
- Not Convenient
- Security Issues

Problem Statement

Major Challenges……

1. High Identification Performance

2. Data Features Design



3. Data Privacy

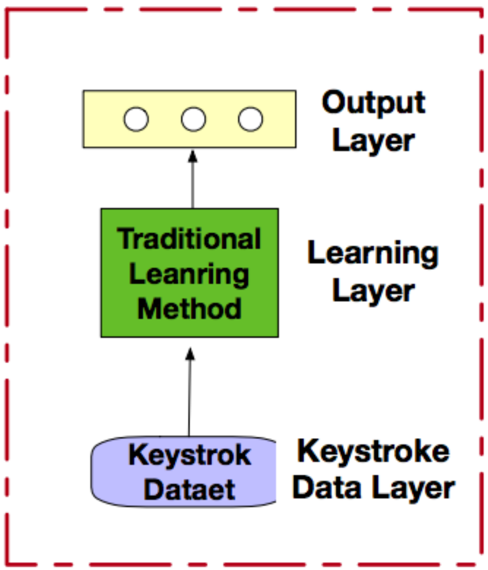
Problem Statement

Feature Design & Selection

Authorization	vs	Identification
Accelerometer Gyroscope Magnetometer Raw touch event Tap gesture Scale gesture Scroll gesture Fling gestur Key press on virtual keyboard …		Accelerometer Tap gesture Key press on virtual keyboard

Problem Statement

Solution I : Single-view Traditional Learning

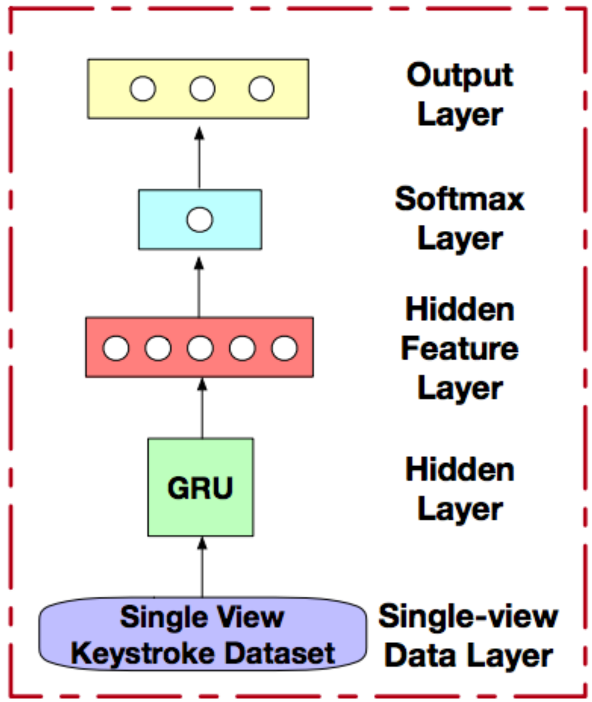


Multi-class Traditional Learning:

Support Vector Machine
Decision Tree
Random Forest
Logistic Regression

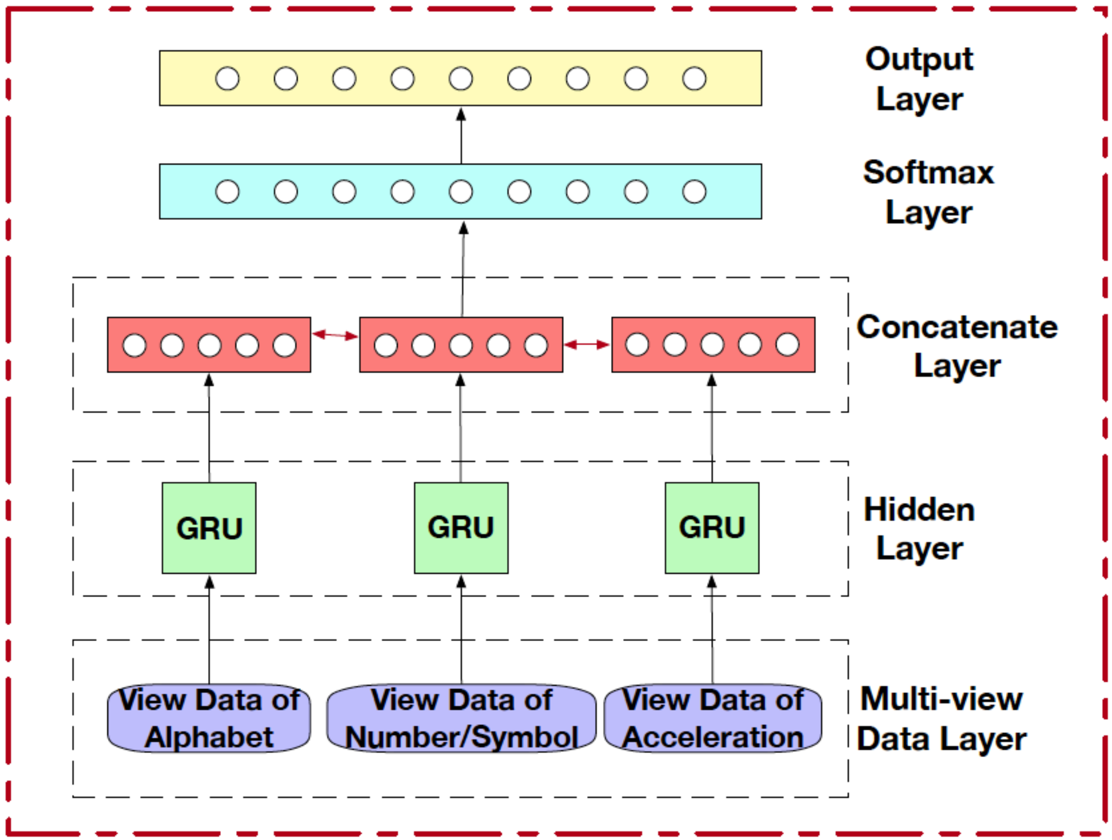
Problem Statement

Solution II : Single-view Deep Learning

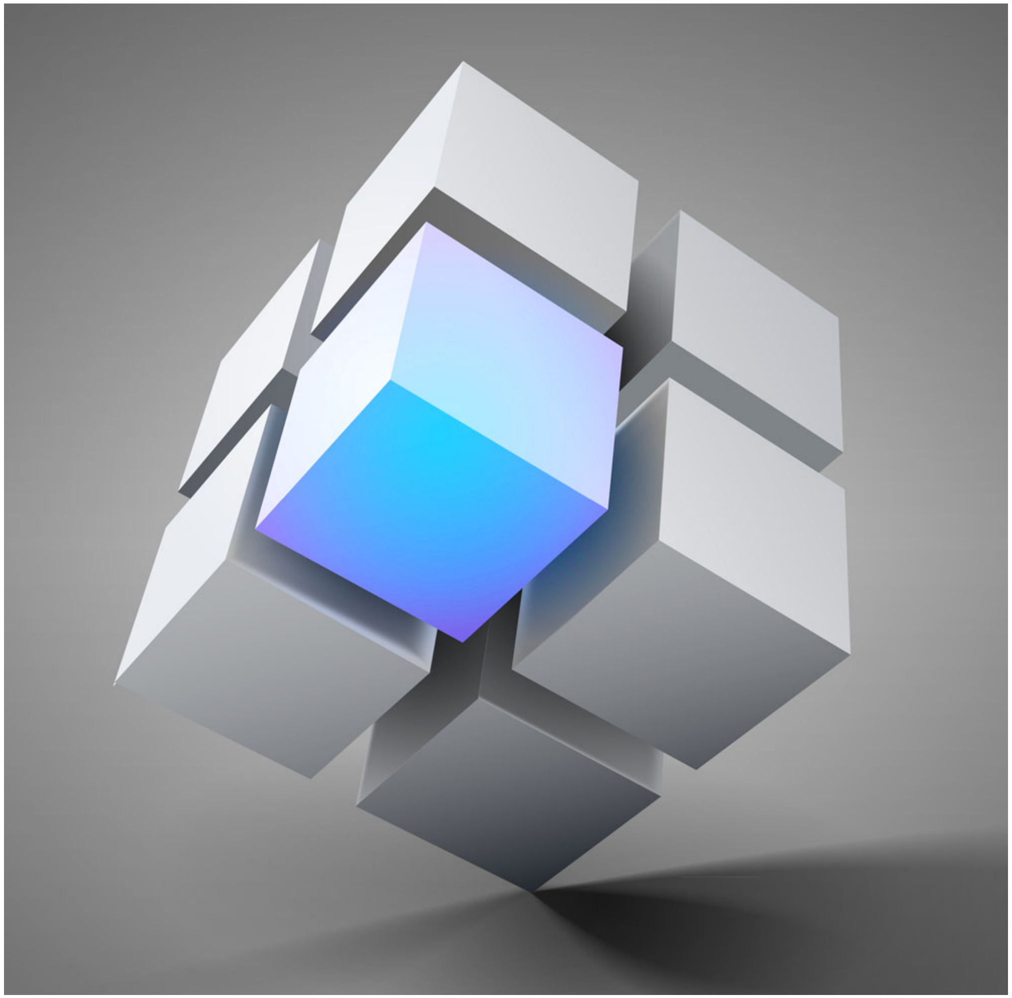


Problem Statement

Solution III : Multi-view Deep Learning



OUTLINE



1 Problem

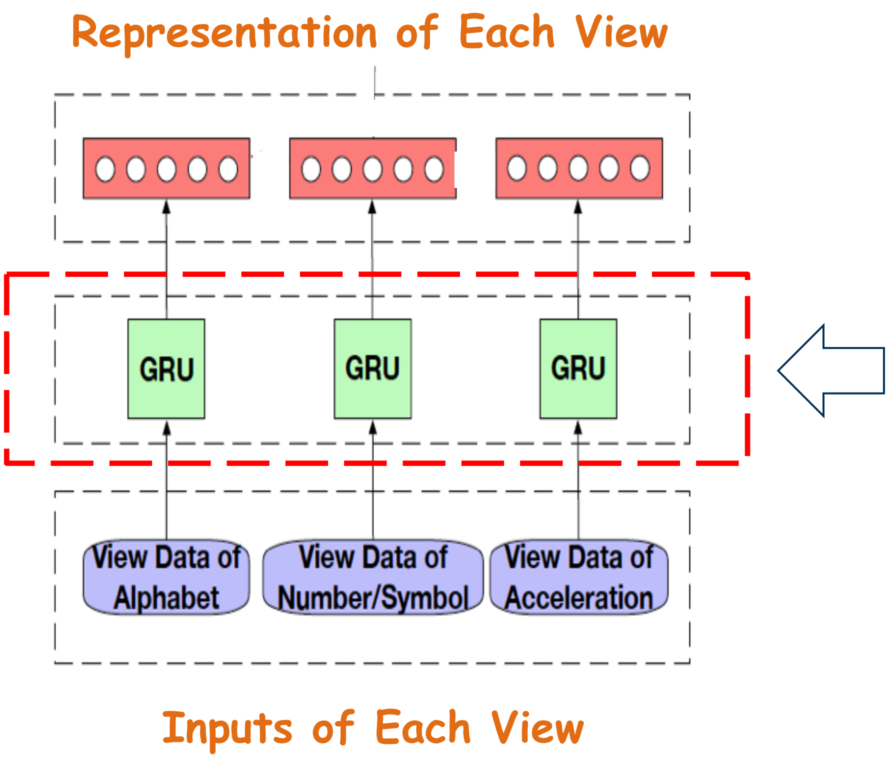
2 **Methodology**

3 Experiments

4 Conclusions

Multi-view Multi-class Deep Learning

Step I : Auto-encoder for Each View



A GRU is formulated:

$$z_t = \sigma_g(W_z x_t + U_z h_{t-1})$$

$$r_t = \sigma_g(W_r x_t + U_r h_{t-1})$$

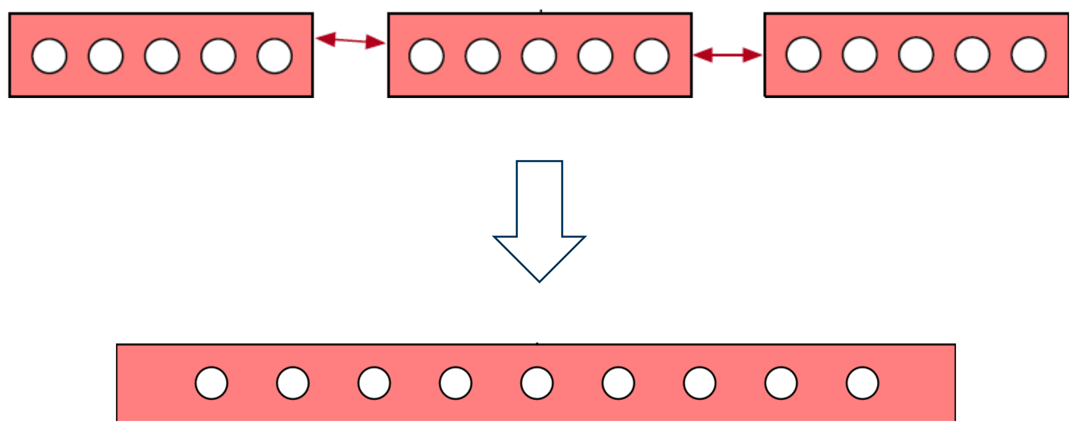
$$\tilde{h}_t = tanh(W x_t + U(r_t \odot h_{t-1}))$$

$$h_t = z_t \tilde{h}_t + (1 - z_t) h_{t-1}$$

$$\sigma_g = 1/(1 + e^{-x})$$

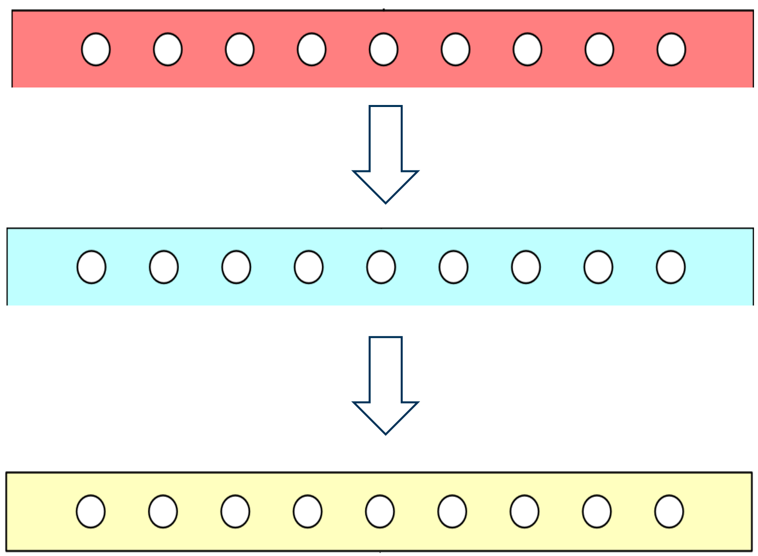
Multi-view Multi-class Deep Learning

Step II : Concatenate Representations of Each View



Multi-view Multi-class Deep Learning

Step III : Softmax & Output



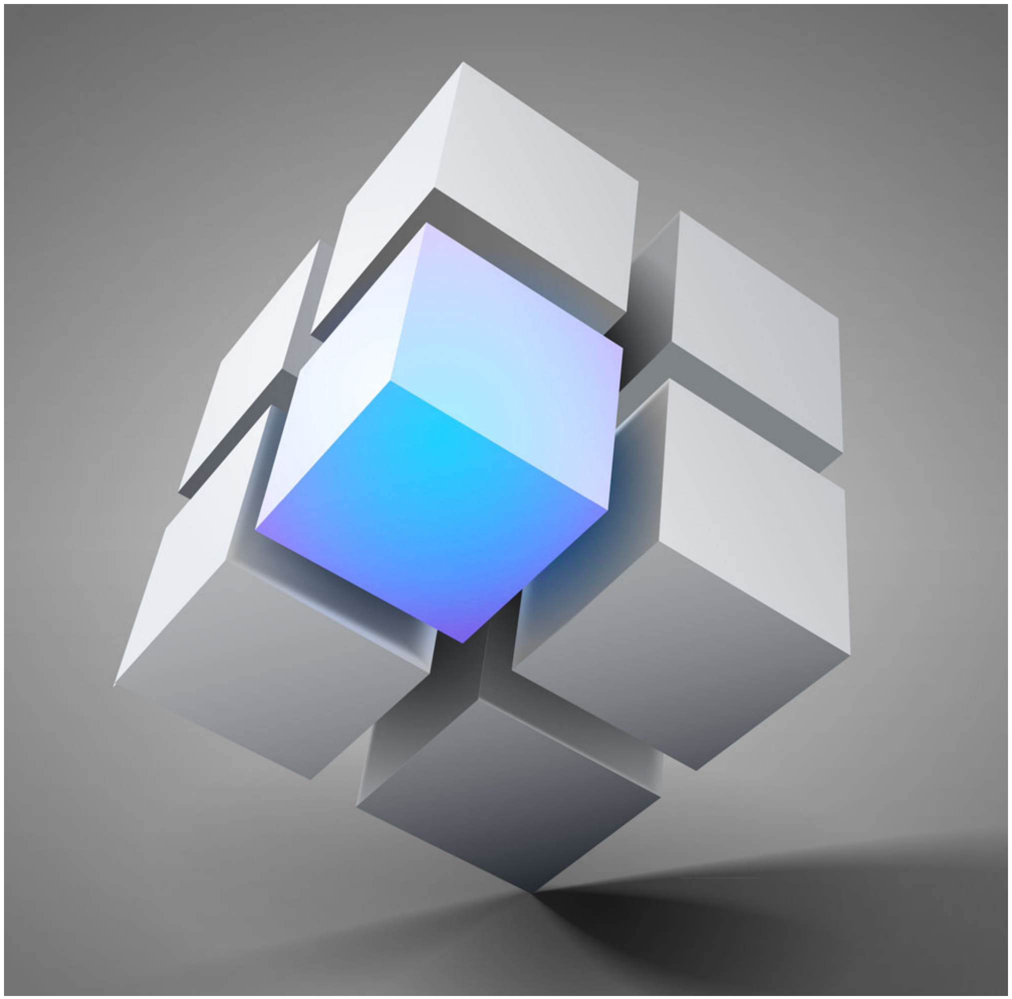
Softmax Function

$$\sigma(\mathbf{z})_j = \frac{e^{z_j}}{\sum_{k=1}^{K} e^{z_k}} \quad \text{for } j = 1, \ldots, K.$$

Multi-class Output:

[0,0,0,1,0,…,0]: single one value
Result: Index of 1 is the multi-class

OUTLINE



1. Problem
2. Methodology
3. **Experiments**
4. Conclusions

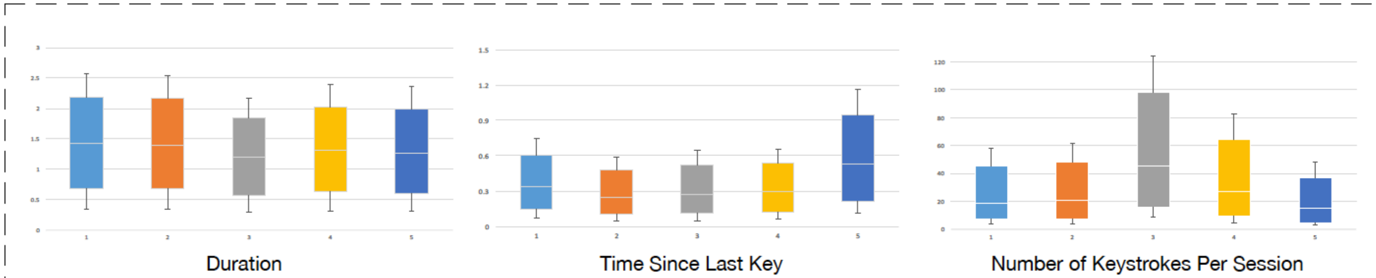
Experiments

Datasets

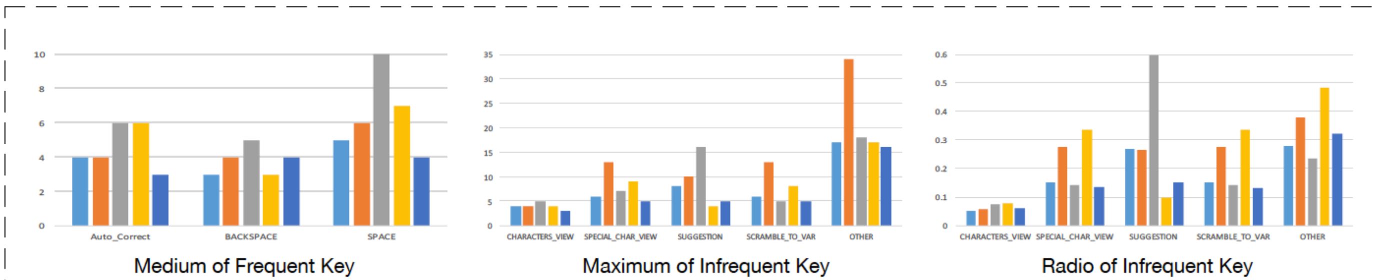
- 40 Volunteers
- 26 of 40 Active Users (17 females and 9 males)
- 8 Weeks
- 11 – 63 years old
- Minimum: 29 Maximum: 4702 Times Usage of the Phone

Experiments

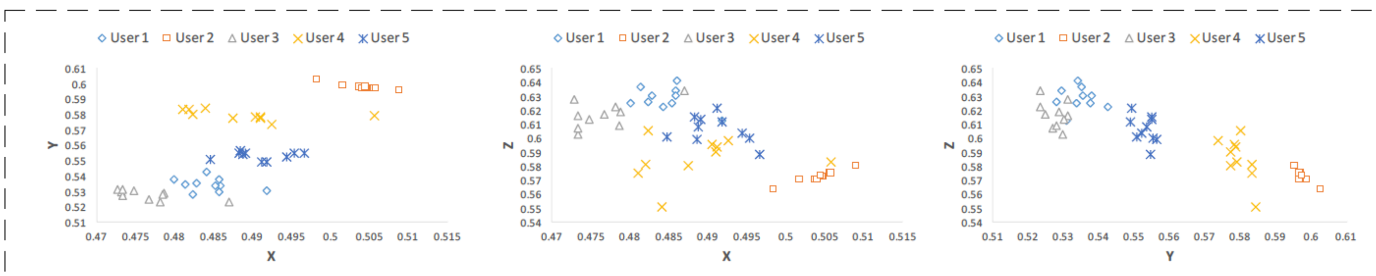
Pattern Analysis



View of Alphabet



View of Symbol/Number



View of Acceleration

Experiments

Results

Table 1. Results of DEEPSERVICE and Baselines

	5		10		26	
Method	Accuracy	F1	Accuracy	F1	Accuracy	F1
LR	66.88%	66.85%	44.25%	45.31%	27.44%	30.26%
SVM	68.18%	68.13%	44.39%	45.12%	30.33%	31.90%
Decision Tree	68.21%	67.50%	53.50%	52.85%	43.37%	42.42%
RandomForest	87.59%	87.42%	77.05%	76.59%	67.87%	66.31%
Deep Single View	82.64%	82.48%	78.27%	78.33%	61.26%	63.11%
DEEPSERVICE	**93.50%**	**93.51%**	**87.35%**	**87.69%**	**82.73%**	**83.25%**

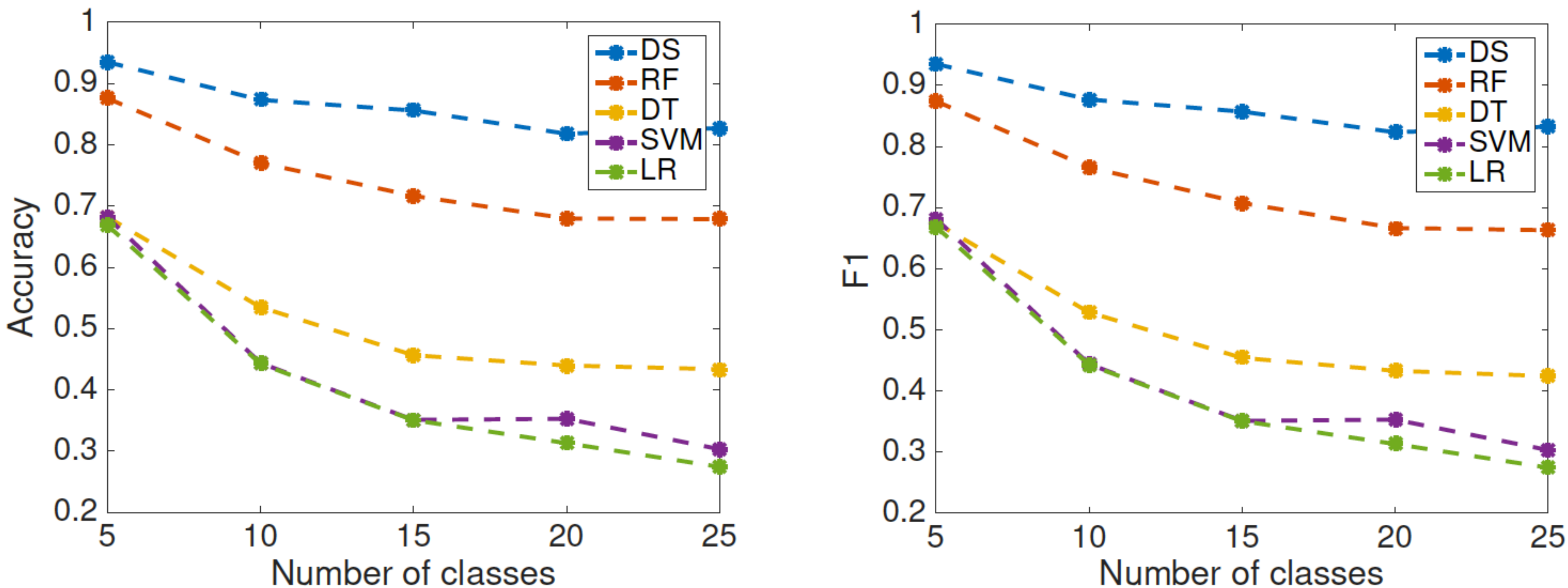
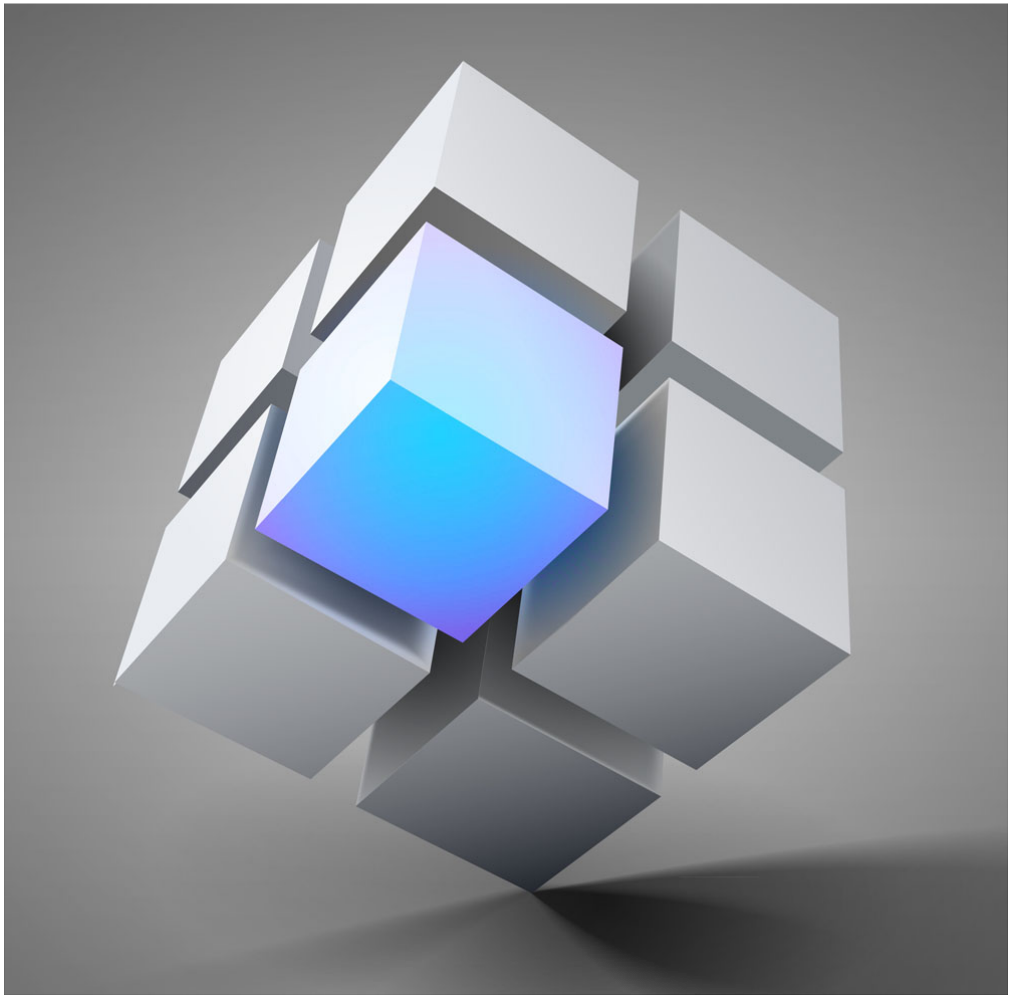


Fig. 5. Results with Incremental Number of Classes (Users)

OUTLINE



1. Problem
2. Methodology
3. Experiments
4. **Conclusions**

Conclusions

We have shown that DEEPSERVICE can be used effectively to identify multiple users. Even though we only use the accelerometer in this work, our results show that more views of dataset can improve the identification performance.

- DeepService is the first system for mobile user identification
- DeepService is the best model for multi-view multi-class dataset
- DeepService takes about 0.657 ms per session which shows its feasibility of real-world usage

Thank you !