Recognize Keystrokes on Touch Screen Using Smartphone Sensors

Zhongze Tang, Zichen Zhu, Weijia Sun
{zt67, zz313, ws368}@scarletmail.rutgers.edu
Advisor: Prof. Yingying Chen
RUTGERS THE STATE UNIVERSITY OF NEW JERSEY

Goal

- ❑ Present an attack that recognizes what's the user's input on an Android smartphone's touch screen by only using the sensors data, which can be collected easily without any permissions.
- ❑ Show that sensor data should be considered as a kind of user privacy as well. Hope this attack can arouse vendors' attention to importance of data privacy.

Motivations and Objectives

- ❑ Motivations
  - Many APPs have access to sensor data nowadays.
  - High risk of data privacy leakage
- ❑ Objectives
  - Implement an APP disguised as a health&fitness APP to collect sensor data at the background
  - Train and use the CNN model to analyze the sensor data to infer the user's input
  - Arouse the public's attention to the serious of data privacy

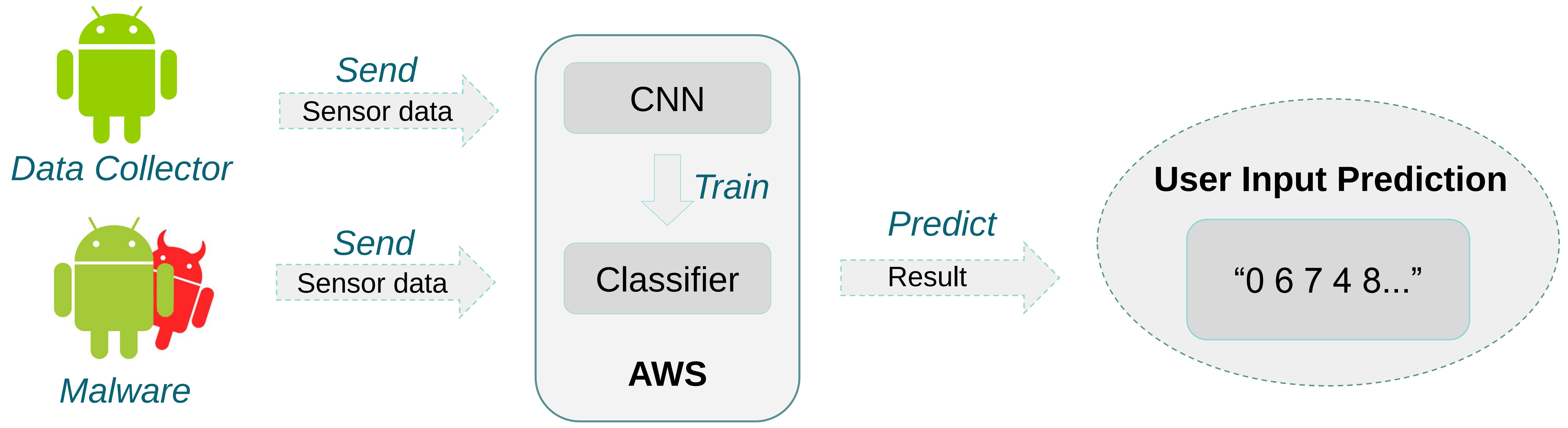
Research Challenges

- ❑ The movements between two touches are small and quick.
- ❑ The sampling rate might be limited because background APP has lower priority.
- ❑ Too much useless sensor data, hard to find out whether it is a touch on the screen or not.
- ❑ How to choose the features to train the CNN model

Acknowledgement

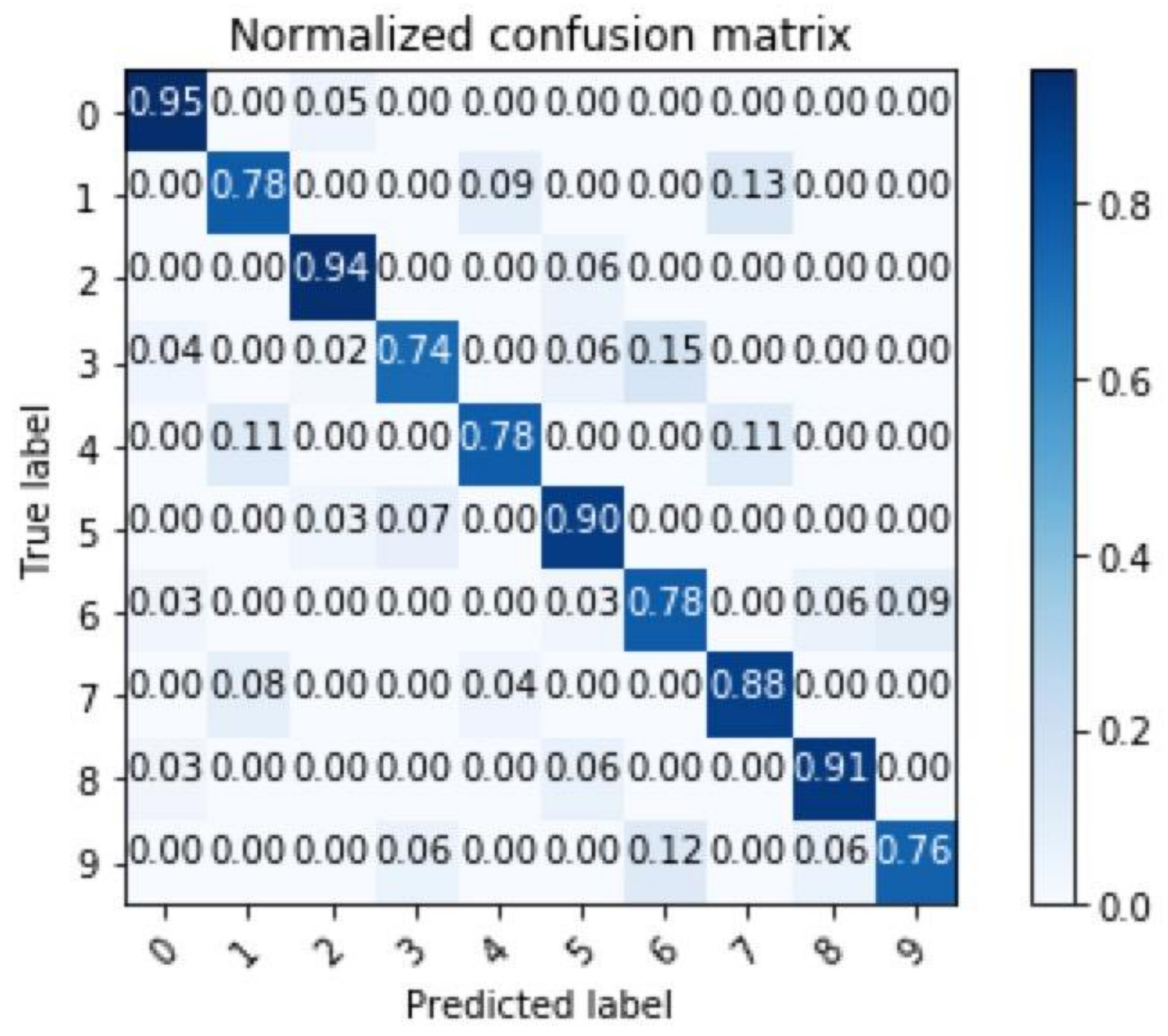
We would like to thank our advisor Prof. Yingying Chen and her Ph.D. student Chen Wang. Thanks for their guidance and companionship.

Methodology

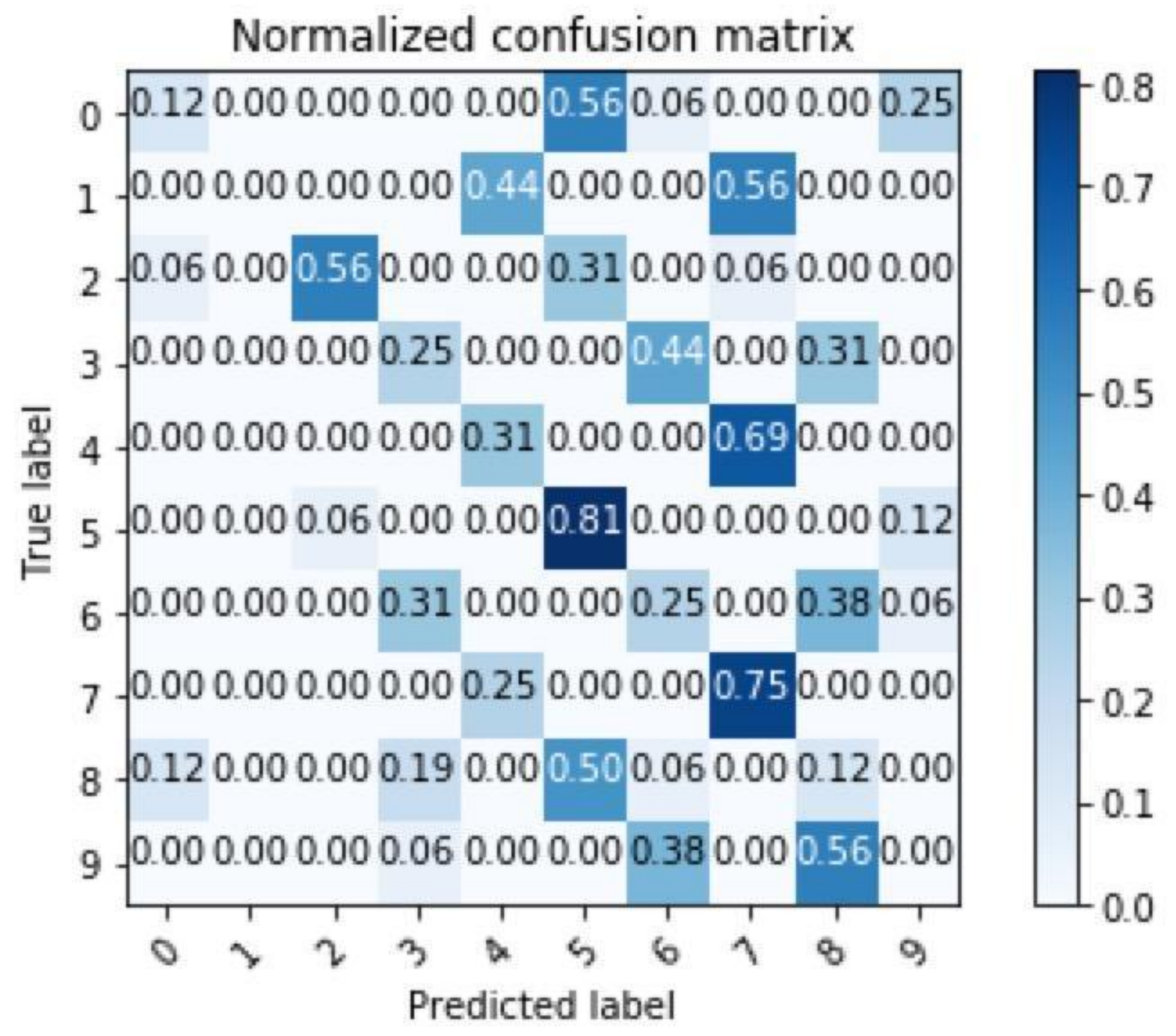


- ❑ Write an APP to collect the training data
- ❑ Machine learning based on TensorFlow
- ❑ CNN architecture: Input->Conv->Conv->Pool->Conv->Conv->Pool->Fully Connected->Fully Connected->Fully Connected->Output->Argmax or Softmax
- ❑ Final model deployed on APP and AWS server

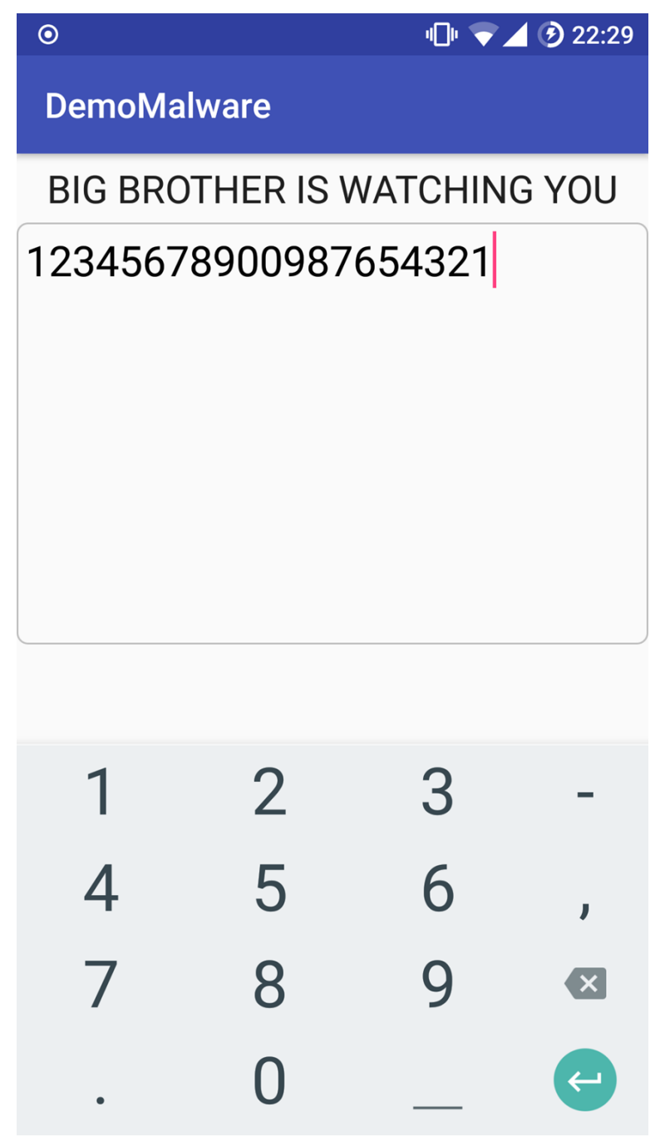
Results



Normalized confusion matrix (cross-valid data)



Normalized confusion matrix (with real data)



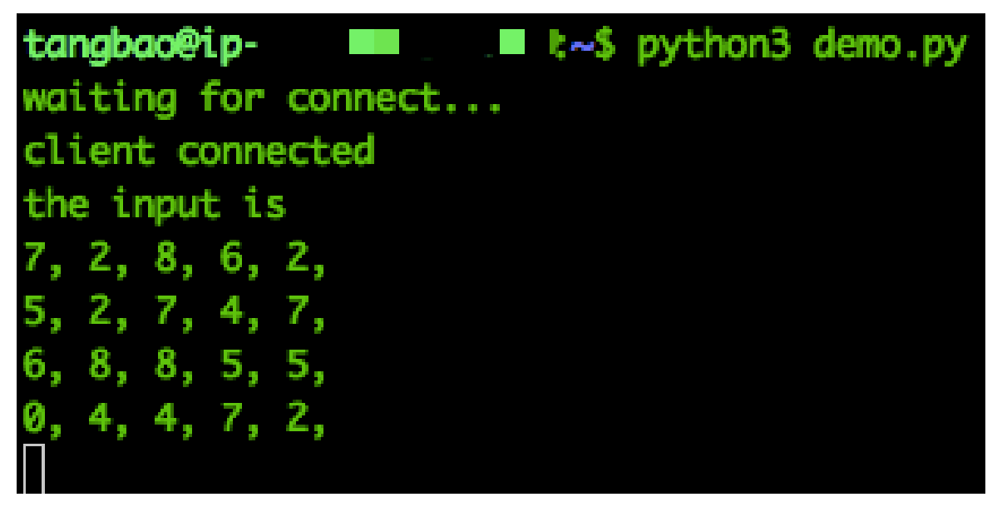
22:29

DemoMalware

BIG BROTHER IS WATCHING YOU

12345678900987654321

Malware Demo



```
tangbao@ip-[redacted]~$ python3 demo.py
waiting for connect...
client connected
the input is
7, 2, 8, 6, 2,
5, 2, 7, 4, 7,
6, 8, 8, 5, 5,
0, 4, 4, 7, 2,
```

Prediction result from remote server

The second figure indicates that we can infer user's input from the sensor data. Although the accuracy is only 60%, the result shows a considerable correlation to the real input. We successfully prove that the sensor data should be considered as a kind of user privacy, which is a more important thing.

References

[1]Owusu, E., Han, J., Das, S., Perrig, A., & Zhang, J. (2012). ACCessory. Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications - HotMobile 12. doi:10.1145/2162081.2162095
[2]Al-Haiqi, A., Ismail, M. & Nordin, R. On the Best Sensor for Keystrokes Inference Attack on Android. Procedia Technology 11, 989–995 (2013).