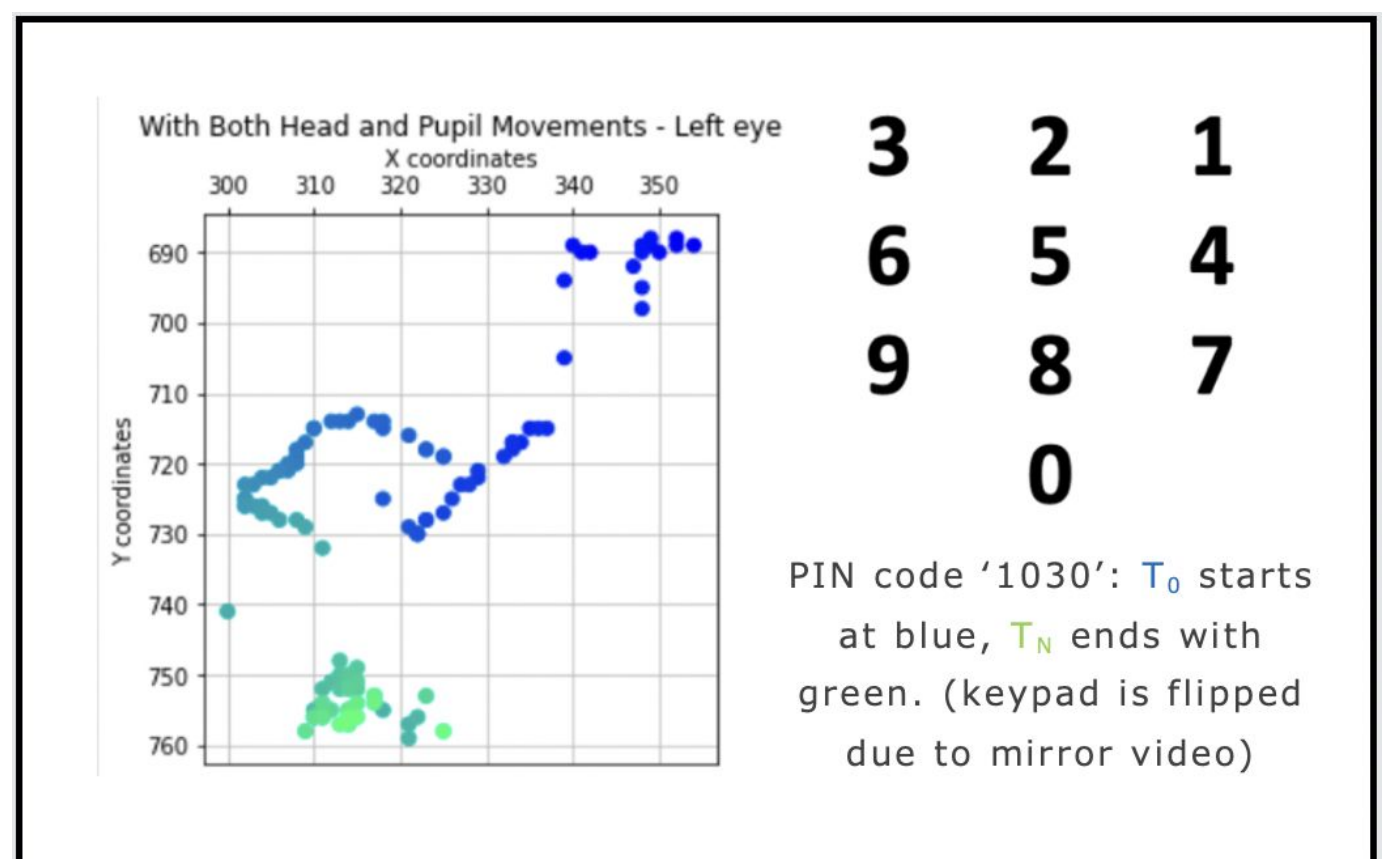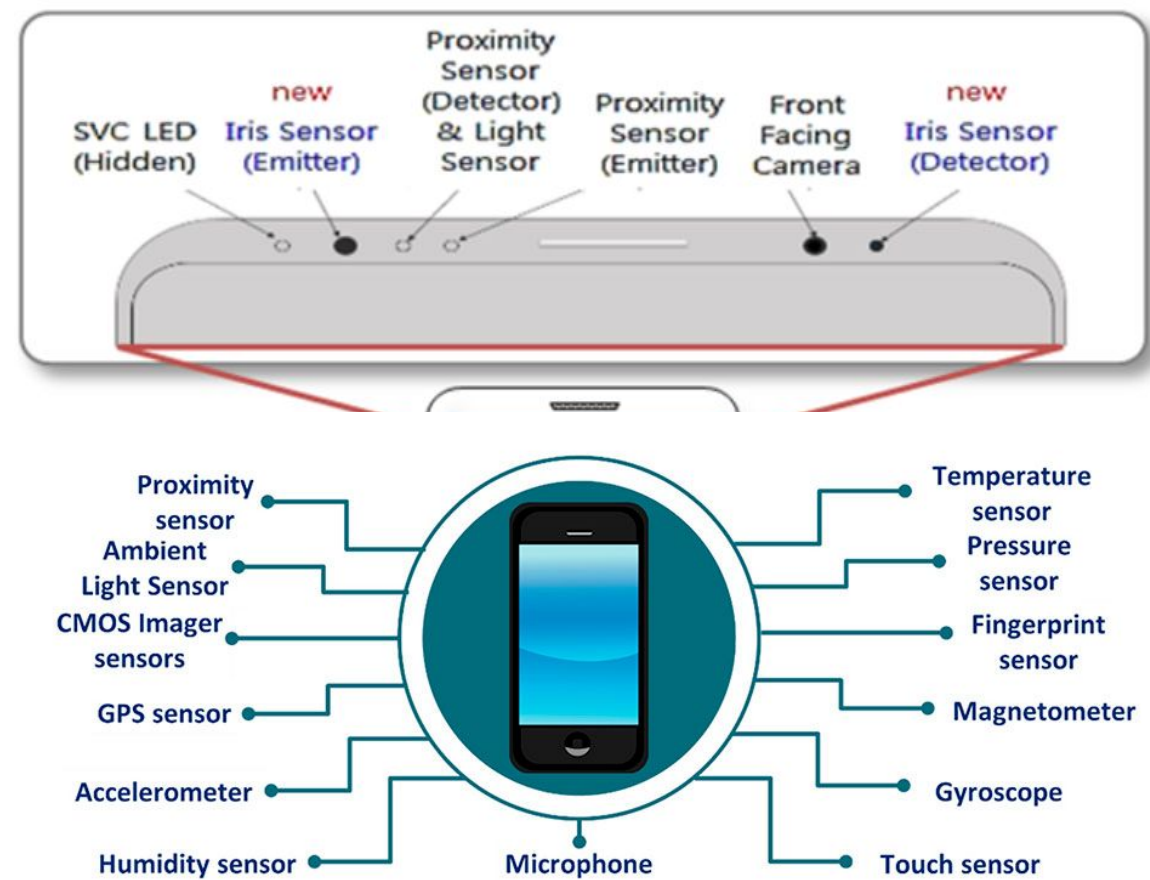# SCSE21-0299 Machine Learning for Attacking Gesture-Based Phone Unlocking

Final Year Project

Student: Kumar Vembu Swathi   Supervisor: Dr Thomas Peyrin

With Both Head and Pupil Movements - Left eye

PIN code '1030': T_0 starts at blue, T_N ends with green. (keypad is flipped due to mirror video)

Project Objectives:

The use of smartphones in our daily lives has increased immensely with the rapid development of technology. Nevertheless, our increasing reliance on smartphones for our day-to-day activities raises some security concerns. Today's smartphones are equipped with various devices like cameras, accelerometers, gyroscopes, and other sensors. Some applications we use have access to these devices without our knowledge. Side-channel attacks exploit this information to obtain sensitive information such as PIN codes. As the victims type their PIN codes, side channels may leak information such as the variation of light, the orientation of the phone, and even coordinates of their eyes and heads. Machine learning and deep learning techniques can be applied to either the sensor or camera data to retrieve PIN codes with good accuracy. In this project, we will process, analyze, and combine the various types of side-channel information to train a model that can retrieve PIN codes more accurately.

Different experiments and model training setups were utilized to determine whether a given digit exists in a pin code. Experiments included feature selection, padding, clustering, etc.

Digit	Accuracy for Decision Tree Classifier
0	55%
1	54%

The baseline or random accuracy for digit is around 33%.Using different techniques, the accuracy is able to improve by over 20% foe every digit. Based on the literature analysis, the results obtained are conclusive and are of good standard. Future works will focus on using these results to retrieve the entire PIN code sequence.