Smartphone Authentication using Soft Biometrics

Radhika Bailurkar 2019430003
Faculty Incharge: Prof. Nataasha Raul

Motivation

As the number of smartphone users have raised, there arises a need for secure authentication. These smartphone companies provide various authentication techniques like PIN, password, fingerprint scanner and face scanning. But there was no mention of continuous authentication of smartphones. Some research papers have proposed the idea of continuous authentication of users using biometrics which deal with behavioral characteristics of user like the tapping, scrolling and swiping on the touch screen. This study focuses on continuous authentication of smartphone user on touch screen medium.

Objectives

1. To study basics of continuous authentication on smart-phone touch screen.

2. To do comparative analysis of different methodologies.

3. To provide solution, to design more efficient authentication system for user using smartphone touch screen.

Basics of Biometrics

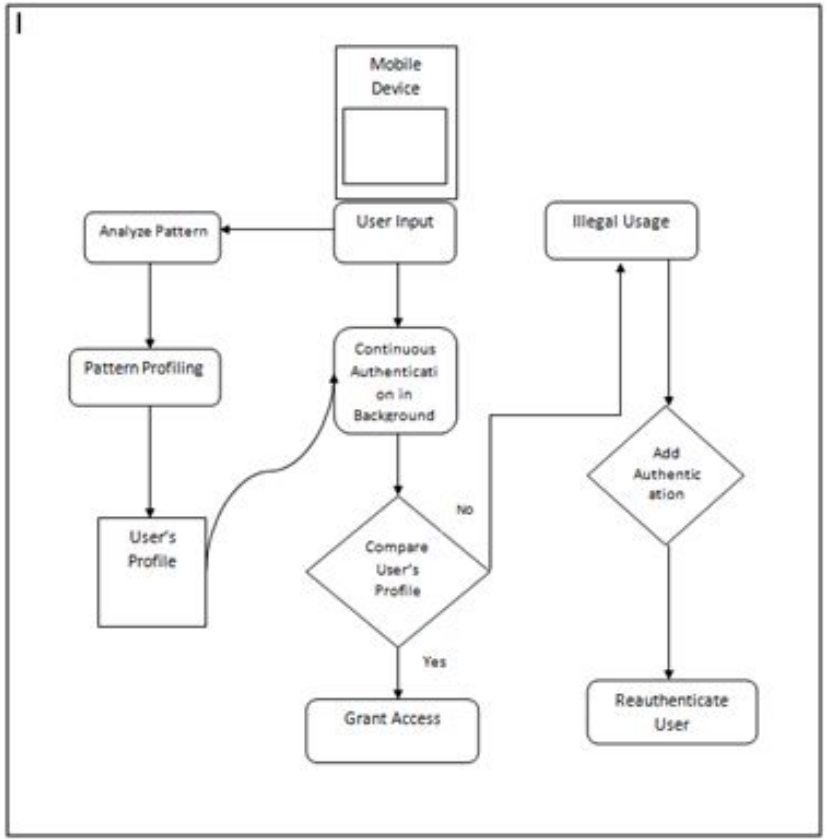
- Physical Biometrics focuses upon examining the biological and the physiological features of the human being. These unique features include the shape of the hand, finger, and face, and the structure of the eye.
- Behavioral Biometrics focuses upon examining the non-biological or the non-physiological features of the human being.
- Soft biometrics provide ancillary information but are not fully distinctive and permanent, so these features cannot provide a reliable person recognition. However, such ancillary information still can be used as a secondary information to complement the primary biometric traits (face, iris, etc.), and these features can be classified to physique (e.g., color skin, gender, ethnic origin), clothing (e.g., clothes' color), or accessories (e.g., glasses, hat).

Gaps

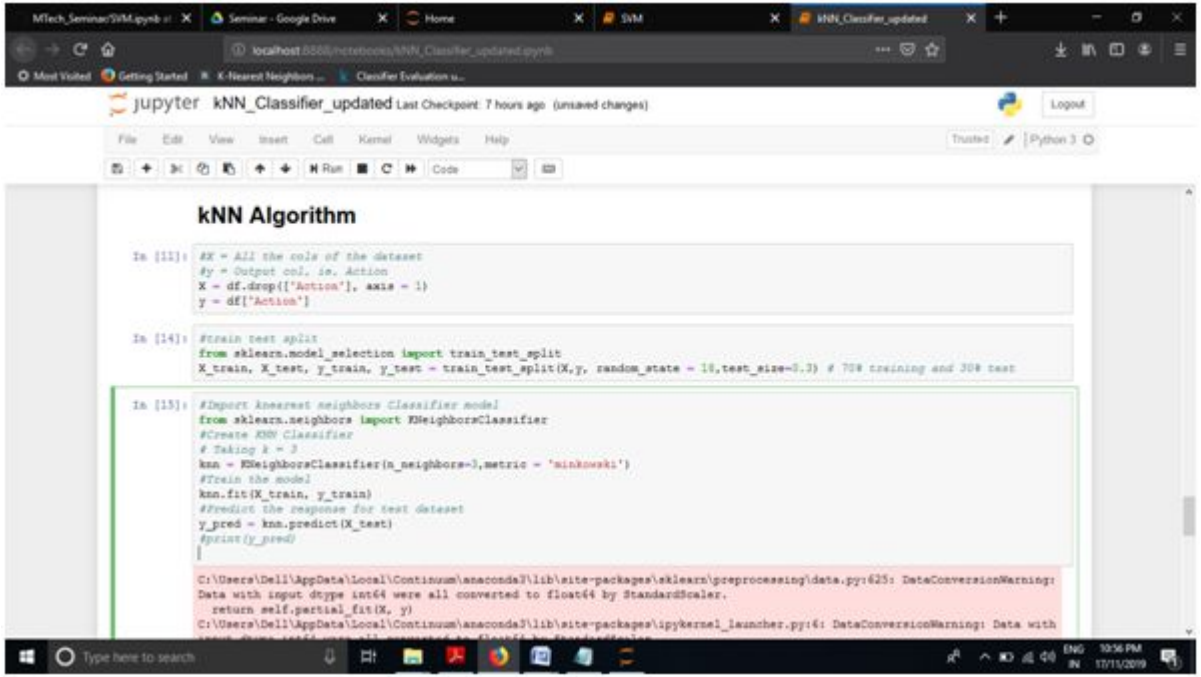
- In this study, we report that combining multiple features gives better results than using each single feature alone.
- Touch based results vary for different Mobile Model. For instance, the screen of different phones have slightly different dimensions.
- Sometimes an impersonator might mimic the touch behaviour of another user.(For example, he can be a friend, coworker or a family member)
- Increase the feature space by including a categorical variable that records values like ‘read e-mail’, ‘write e-mail’, ‘browse’, ‘control music player’.

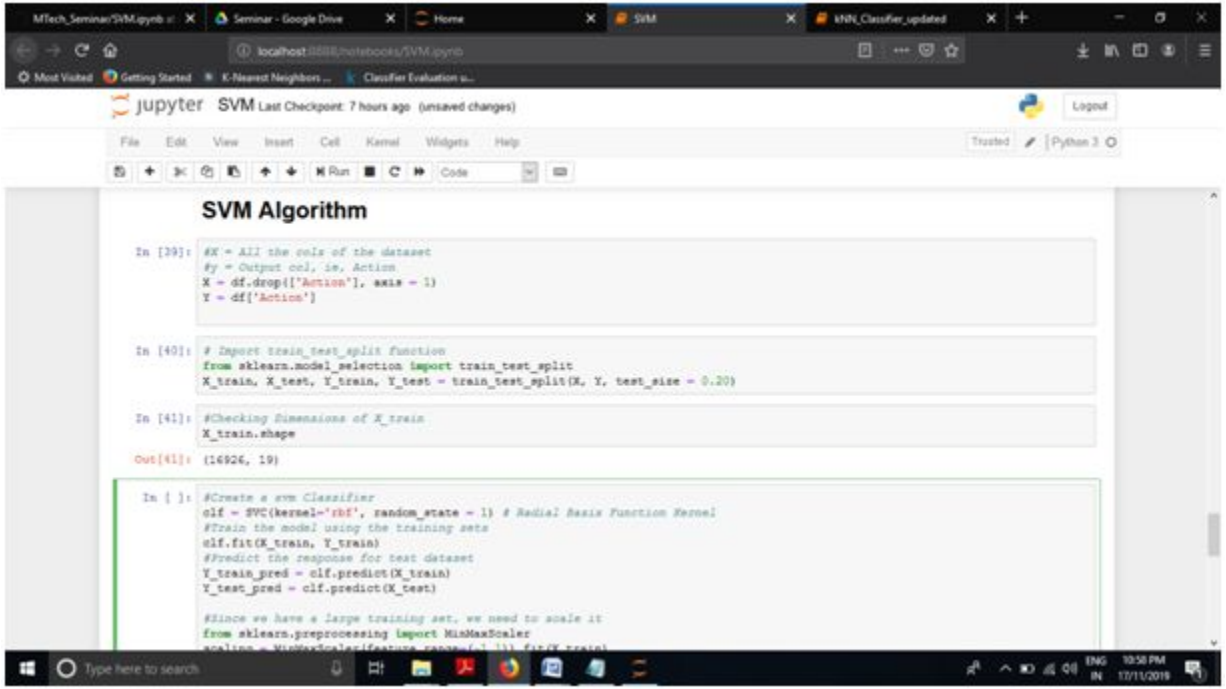
- Influence of sample size

Workflow Model



Implementation




jupyter SVM Last Checkpoint: 7 hours ago (unsaved changes)
File Edit View Insert Cell Kernel Widgets Help
SVM Algorithm
In [39]: #X = All the cols of the dataset
#y = Output col, ie, Action
X = df.drop(['Action'], axis = 1)
Y = df['Action']
In [40]: # Import train_test_split function
from sklearn.model_selection import train_test_split
X_train, X_test, Y_train, Y_test = train_test_split(X, Y, test_size = 0.20)
In [41]: #Checking Dimensions of X_train
X_train.shape
Out[41]: (16926, 19)
In [ ]: #Create a svm Classifier
clf = SVC(kernel='rbf', random_state = 1) # Radial Basis Function Kernel
#Train the model using the training sets
clf.fit(X_train, Y_train)
#Predict the response for test dataset
Y_train_pred = clf.predict(X_train)
Y_test_pred = clf.predict(X_test)
#Since we have a large training set, we need to scale it
from sklearn.preprocessing import MinMaxScaler

Accuracy

TouchAlytics Dataset	kNN(k = 5)	SVM(kernel = rbf)
21158 rows and 20 columns	92.407%	91.918%

References