**Chapter 7**

# Conclusion

Security and privacy are major concerns for the users when using any electronic device. We have explored how the sensors are used in the smartphones and the permissions and security related to these sensors. There were no permissions asked when using any of the motion sensors on the phone. This vulnerability was exploited to know about the user input patterns to get hold of his/her PIN for the phone. The targeted smartphone operating system is Android as a majority of the people use Android phones. This does not mean that iOS provides any special permission requests before using these sensors. The only difference is that of how the background processes are handled by them.

By exploiting the sensors used on smartphones, it is possible to develop a single-digit classification machine learning model to predict the PIN entered by a user to unlock the phone. Different types of pre-processing methods and different classification models were used in method 1, where maximum accuracy achieved for on-hand data collection method is 42.5% using a random forest classification model, in-hand data collection method is 42.47% using a support vector machine model, and for merged data, it is 39.89% using K-Nearest Neighbours.

In method-2, we eliminated all the models that were not showing good accuracies from method-1. We increased the window size for the input file so that it contains all the required data of the path followed by the phone when it is touched. We can observe that the combination of both sensor type, Accelerometer without gravity and gyroscope with a window of 200 each gives a good accuracy for Logistic Regression (64.29%) and Deep learning model (64.99%). Since getting a window of 400ms for a digit in the real-world scenario is not possible every time as the speed of typing may be high for a PIN as it is entered very frequently, the processing of file with larger window size is eliminated.

We can conclude that that the PIN lock of a phone is crackable using these motion sensors to a extent. Out of 50 4-digit PINs, we were able to predict at least one digit correct for 38 4-digit PINs. The prediction accuracy of 28.36% for 200 digits from the Logistic Regression model is significantly higher than the primary cracking method of trying out every combination.

On comparing our results with [15] and [17], it can be observed that the model accuracies are not coming up to the same mark due to the different methods of data collection (71.82% and 83.7%) . However, the exploitation of sensor data and their results are absent in [15] and [17]. Therefore, the comparison cannot be made on that account. The further exploitation of PIN from the phone and processing the file using only the graph with no proper time stamp reduces the accuracy of the already trained model of ours. Deep learning model did not perform well with the fresh new data because of the small size of the dataset.

Observing the graph in the figure above, we can say that, by increasing the size of the dataset for training, we can improve predicting power of a model. We can see a significant rise in accuracy in Deep learning model and support vector machines.

As the Accelerometer without gravity and Gyroscope sensors are not affected by the initial position of the phone in 3D space, the training dataset can be extended by profiling different ways of holding the phone alone. This method is flexible to accommodate longer PIN length (greater than 4) and can also be scaled up to be used not only to extract PIN used for locking the phone but to any internet banking apps and websites.

There are certain limitations attached to this, such as the person needs to install this app and open it once in order to start the background service. The app should provide functionalities that user trusts, and allows it to be run in the background. The internet connection to the phone is a must to upload the raw sensor data files to be accessed remotely.