**Name:** Sowndarya Krishnamoorthy

**Student ID:** 104654482

**Project Description**

**USER AUTHENTICATION USING MOUSE DYNAMICS**

Problem Statement

To protect a set of users from the illegitimate use of their accounts, the attributes of how they use their mouse is taken into account for authorizing the user. During their work, these users usually sign into remote servers with their remote desktop client. A network monitoring device set between client and remote server inspects all traffic using RDP protocol and records the mouse interaction sent by the user transmitted from the client to the server during the remote session.

Unfortunately, if the user account is stolen and if the server suspects illegitimate access by the person who is not the legit owner of the account, the server inspects the mouse behaviour of the user recorded from the network monitoring device. It is assumed that the way a person moves their mouse is particular to them and can be utilised as a sort of behavioural biometric identifier. Thus, typical patterns of each user are identified using mouse movement data (timing and position information) and stolen accounts can be retrieved.

Dataset

The training dataset has different users with data recorded during various remote sessions that are carried out by legitimate owners of the respective user accounts. The test dataset has different users with data recorded for shorter remote sessions; however, the true identity of the user in the test session is unknown.

Approach

The dataset has labelled samples hence classification machine learning techniques will be applied to classify the problem and authenticate the users based on their mouse behaviour. The features are the recorded timestamp, client timestamp, button, state, X co-ordinate and Y co-ordinate which has to be inspected for identifying a user for a particular web session. The classifier classifies the class if the user is legitimate or illegitimate. The captured area under the ROC curve (AUC) tells how unlikely it is that the remote session was carried out by the respective user. Various pattern recognition techniques will be applied on the large dataset to classify and identify the user and obtain the best accuracy to find the legitimate user for respective sessions. Support Vector Machines (SVM) can be used to classify based on the angle based metrics for better accuracy and quick response. The data is initially projected into higher dimensional space, after which dimensionality reduction procedures are applied to classify the dataset better.