# Behavior & Biometrics Based Masquerade Detection Mobile Application

P. Chandrasekara , S. Rajapaksha , H. Abeywardana , P. Sanjeevan,
K. Y. Abeywardena

*Faculty of Computing, Sri Lanka Institute of Information Technology, Malabe, Sri Lanka*

Mobile phone has become an important asset when it comes to personal security since one's mobile is now a virtual safe for that person. This is due to the sensitivity of the details which are stored in these devices. To protect the information inside a mobile phone the manufacturers use conventional technologies such as password protection, face recognition or finger print protection. Nevertheless, it is clear that these security methods can be bypassed by several other techniques as shoulder surfing, finger print or face recognition by pass with 3D printing. Due to these concerns post authentication is an increasingly discussed topic in the security domain. However, there are very few applied researches done on the post authentication of mobile platforms. In order to protect the phone from an unauthorized user a novel method is proposed by the authors. The aim of the research is to detect the illegitimate user by monitoring the behavior of the user. In order to detect the behavior four main parameters are proposed. Namely, Key stroke dynamics using a customized keyboard, location detection, voice recognition and App usage. Initially machine learning is used to train this mobile application with the authentic user's behavior and they are stored in a central database. After the initial training period the application is monitoring the usage comparing it with the existing data of the legitimate user. Another unique feature is the inbuilt prevention mechanism which is designed to be executed when an illegitimate user is detected. The entire storage content will be encrypted and a current location alert along with a captured photo of the intruder will be sent to a pre-defined account of the real user in a cloud platform. The real user can log into the account remotely and obtain the phone's location and the photo of the intruder. Furthermore, this application is proposed as an inbuilt application in order to avoid the deletion of app or uninstallation of the app by the intruder. With this proposed post authentication application "AuthDNA", a user is able to protect sensitive information of the mobile device in case of theft and bypassing of initial authentication.

*Keywords: Machine Learning; Authentication; Encryption; Voice recognition; Cloud Storage.*

[1]Corresponding author.
*E-mail address:* sammani.rajapaksha5@gmail.com