Chapter 2
Machine Learning as an Enabler of Continuous and Adaptive Authentication in Multimedia Mobile Devices

José María Jorquera Valero
Universidad de Murcia, Spain

Pedro Miguel Sánchez Sánchez
Universidad de Murcia, Spain

Alberto Huertas Celdran
https://orcid.org/0000-0001-7125-1710
Waterford Institute of Technology, Ireland

Gregorio Martínez Pérez
Universidad de Murcia, Spain

ABSTRACT

Continuous authentication systems allow users not to possess or remember something to authenticate themselves. These systems perform a permanent authentication that improves the security level of traditional mechanisms, which just authenticate from time to time. Despite the benefits of continuous authentication, the selection of dimensions and characteristics modelling of user's behaviour, and the creation and management of precise models based on Machine learning, are two important open challenges. This chapter proposes a continuous and adaptive authentication system that uses Machine Learning techniques based on the detection of anomalies. Applications usage and the location of the mobile device are considered to detect abnormal behaviours of users when interacting with the device. The proposed system provides adaptability to behavioural changes through the insertion and elimination of patterns. Finally, a proof of concept and several experiments justify the decisions made during the design and implementation of this work, as well as demonstrates its suitability and performance.

DOI: 10.4018/978-1-7998-2701-6.ch002

1. INTRODUCTION

Continuous authentication systems provide a higher level of security (Gupta, Yamaguchi, & Agrawal, 2018) than traditional authentication systems. This is due to traditional systems rely on passwords, patterns or PINs, which can be lost, forgotten or discovered by an attacker. Additionally, many times, users use the same authentication credentials to different services, which is a security problem in case of being stolen. In this sense, continuous authentication systems allow users not to possess or remember something to authenticate themselves in a device or system. This feature improves the user's quality of experience because it allows performing certain operations that require a prior authentication in a faster and easier way. This is because continuous authentication systems are responsible for performing authentication without requiring new credentials. Apart from the different traditional security techniques provided by current mobile devices, the fact of being able to authenticate continuously a user provides a higher level of security. Besides, it allows users to interact with applications, which require the previous authentication, in a more simple, agile and enjoyable fashion.

Multimedia mobile devices (Jararweh et al., 2017) are one of the most important subjects where continuous authentication can be applied. The use these devices has become a daily activity for the majority of the population of industrialized countries, for example, there are 2.71 billion smartphone users in the world today (2019) (Deyan, 2019). Within this wide range of multimedia mobile devices, there is a huge variety in terms of usage, from a private and personal usage such as social networks, take pictures or videos, online banking or entertainment, to a professional usage as the generation of invoices or consult customer data. The sensitive information stored in the multimedia devices and its usage is extremely important (Huertas, Gil, García & Martínez, 2016) so several knowledge managements measures must be taken. The private information should be protected, so, most users restrict access to this information by controlling the access to the device. For that, it is necessary to make use of authentication mechanisms.

The idea of using the authentication mechanisms based on users' actions (behavioural biometrics) arose as a potential solution to improve the security (Gupta, 2018) of multimedia mobile devices. These mechanisms allow analysing continually the behaviour pattern of the owner of the device. After modelling the user's behaviour, the authentication system creates a behaviour profile associated with this conduct or conducts. Finally, in real time the authentication system evaluates the current behaviour of the mobile device with the stored profile of the owner. According to the numeric output of this evaluation, the system decides if the person using the device is the owner or not. This mechanism is passive, and it does not need any change in the interaction between the user and the device. Note that if processing is done in an external cloud, extra measures should be taken to preserve users' privacy (Olakanmi & Dada, 2019).

Despite continue authentication systems provide a lot of benefits, as previously highlighted, they also present some open challenges that should be solved to have complete and effective systems. Among these open challenges, we highlight the next ones:

- Selection of dimensions and characteristics that allow modelling the user's behaviour accurately and effectively. The combination and selection of both the different device input sources, and dimensions, from which the authentication system obtains information about the user's behaviour, as well as the features that compose these, are one of the main pillars for the correct evaluation of the user's behaviour.