Chapter 13

Continuous User Authentication on Touchscreen Using Behavioral Biometrics Utilizing Machine Learning Approaches

Amany Sarhan

Department of Computers and Control Engineering, Faculty of Engineering, Tanta University, Egypt

Ahmed Ramadan

Department of Computer and Control Engineering, Faculty of Engineering, Tanta University, Egypt

ABSTRACT

Nowadays, touchscreen mobile devices make up a larger share in the market, necessitating effective and robust methods to continuously authenticate touch-based device users. A classification framework is proposed that learns the touch behavior of a user and is able afterwards to authenticate users by monitoring their behavior in performing input touch actions. Two models of features are built; the low-level features (stoke-level) model or the high-level abstracted features (session-level) model. In building these models, two different methods for features selection and data classification were weighted features and PCA. Two classification algorithms were used; ANN and SVM. The experimental results indicate the possibility of continuous authentication for touch-input users with higher promises for session-level features than stroke-level features. Authors found out that using weighted features method and artificial neural networks in building the session-level model yields the most efficient and accurate behavioral biometric continuous user authentication.

INTRODUCTION

With the increasing popularity of mobile computing devices and their applications that access secure services such as banking and other transactions, protecting user data on mobile devices is becoming more and more important day after day. Digital technology is now just a part of life. From online shop-

DOI: 10.4018/978-1-7998-2701-6.ch013

ping to net banking, government transactions and business infrastructure, securing this large amount of data plays a vital role. Data can be secured using various hardware and software technologies (Karnan et al.'s, 2011), (Ouaguid et al.'s, 2018) and (Olakanmi & Dada, A. 2019).

Some common tools are antivirus, encryption, firewalls, two-factor authentication, software patches, updates, etc. Many people have a common misconception that data security is important only for big organizations, governments and businesses and they are only the target of data attackers. Data security is not just important for businesses or governments. Your computer, tablet, and mobile devices could be the next target. Usually, common users get targeted by attackers for their sensitive information, such as their credit card details, banking details, passwords, etc. All the previous lead to the existence of the most famous authentication scheme to protect user data and privacy that is password scheme (Mahfouz et al., 2017, Feng et al., 2012, Zhao et al., 2014, Jouini & Rabai, 2016).

Current applications maintain the privacy of user sensitive data by supporting user authentication at every login. Most mobile device applications today enforce security using traditional text-based password schemes to authenticate a user. However, users often choose weak passwords to make the login process more easy and quick (Jain et al., 2004). This is especially true with touch devices that are rapidly becoming ubiquitous. Findlater et al. (2011) have shown that the speed of typing on fiash glass is 31% slower than a physical keyboard. This typically leads to a shorter password chosen by users to shorten their login time. Choosing the appropriate password puts the user in a dilemma between using an easy-to-remember password and, at the same time, safe password so, most users sacrifice security to guarantee easy and quick login process which is the most frequent action done by touch input mobile devices so there was an urgent need to find other alternative authentication methods to solve this dilemma and give the user a more quick and easy login experience and at the same time doesn't make the user to sacrifice security (Frank et al., 2013).

Other authentication methods that could be better alternatives to a password authentication scheme, such as graphical patterns are most encouraging, but also are vulnerable to attacks, such as trying to discover the residues left on the touchscreen of the device after entering the same pattern many times. In addition to the previously mentioned, the main limitation of traditional security systems is that the user is only authenticated once at the beginning of the session. This authentication process is not performed until the next time the device needs to be unlocked (Karnan et al., 2011). All these problems and limitations lead to using some type of implicit and continuous authentication method to overcome these limitations. According to that, the authentication method needs to be continuous to overcome any attempt to access secured data illegally (Gianni et al., 2017). These methods are not valid in many situations like authentication of a student in an online exam.

In addition to being continuous, the authentication process should be implicit and transparent so that it cannot affect the user activity. In this context several academic and industrial research groups have proposed different solutions to monitor user activity and authenticate him along the time he is using his device. Continuous authentication can be the primary authentication method or an auxiliary fraud detection for higher assurance. It adds an extra reliability to the system and enhances the usability (Eberz and Rasmussen, 2017). Continuous authentication can be implemented using different methods according to hardware and software requirements. For example, we can implement it by setting session time out and ask the user to perform the authentication process which is very annoying to the user. Another method is to record data about how the user uses the device, and make a frequent comparison between this data and the previously recorded data of the same user. This solution is more applicable when we deal with behavioral biometric authentication methods which will be discussed later.