Chapter 4
Application of Machine Learning to User Behavior-Based Authentication in Smartphone and Web

Manoj Jayabalan
https://orcid.org/0000-0002-1599-965X
Liverpool John Moores University, UK

ABSTRACT

Authentication is the preliminary security mechanism employed in the information system to identify the legitimacy of the user. With technological advancements, hackers with sophisticated techniques easily crack single-factor authentication (username and password). Therefore, organizations started to deploy multi-factor authentication (MFA) to increase the complexity of the access to the system. Despite the MFA increasing the security of the digital service, the usable security should be given equal importance. The user behavior-based authentication provides a means to analyze the user interaction with the system in a non-intrusive way to identify the user legitimacy. This chapter presents a review of user behavior-based authentication in smartphones and websites. Moreover, the review highlights some of the common features, techniques, and evaluation criteria usually considered in the development of user behavior profiling.

DOI: 10.4018/978-1-7998-9430-8.ch004

INTRODUCTION

Digital authentication provides a means to secure access to digital information through various technologies. It acts as a prime component in the access control system to mitigate the risk of unauthorized access (Grassi et al., 2017; Jayabalan, 2020). The traditional and most widely used approach to identify the legitimacy of the user consists of supplying a username and password, a system known as Single Factor Authentication. The password is the oldest and predominant authentication factor that exists in the information security world. It is the simplest method to implement and inexpensive, but it is prone to vulnerabilities such as users using weak passwords that are easily cracked, phishing attacks, and other common hacker techniques (Raza et al., 2012). The technological advancements plethora the usage of digital service that requires several authentication factors to be implemented to prevent malicious users. As such, there is a need for organizations to employ Multi-Factor Authentication (MFA) where increased complexity such as using a combination of two or more independent authentication factors (smart cards, biometrics, and security tokens) offers extra security protection (Andrean et al., 2020).

Three-factor authentication using the combination of the above factors can offer greater privacy and security, but as it is more complex, and organizations also have to maintain acceptable efficiency levels, it is a greater challenge to implement. There is an increase in biometric authentication systems in several organizations since these grant access only after validating a subject's unique characteristics (Memon, 2017). Biometric authentication is broadly classified into physiological and behavioral. The physiological biometrics are based on the subject physical properties such as iris, fingerprint, face, and palm. Whereas behavioral biometrics measures the subject unique behavior or patterns from voice, keystroke, mouse dynamics, gait, and system usage, which can uniquely identify an individual (Aupy & Clarke, 2005; Ferbrache, 2016; Meng et al., 2015; Vielhauer, 2006).

The behavioral biometric strike the balance between security and usability via monitoring the user behavior throughout the active session. According to Global Opportunity Report 2017,

Behavioral biometrics analyses specific human behavior with intelligent software, adding a new layer of security to verifying identification that is nearly impossible to replicate, without any additional stress for the user. Products and services in this market are moving digital security beyond simple passwords and pin codes, ensuring that as cybercriminals become more advanced, so too do everyday users (DNV GL AS, 2017).

Addressing Data Privacy Concerns in Digital Emerging Technologies: Strategies and Best Practices

Hanan Aldowah, Shafiq Ul Rehmanand Sohail Ahmed Shahani (2025). *Challenges and Solutions for Cybersecurity and Adversarial Machine Learning (pp. 449-476).*
www.irma-international.org/chapter/addressing-data-privacy-concerns-in-digital-emerging-technologies/382269