Chapter 11
Biometric Authentication Schemes and Methods on Mobile Devices: A Systematic Review

Akon Obu Ekpezu
https://orcid.org/0000-0002-9502-1052
Cross River University of Technology, Cross River, Nigeria

Enoima Essien Umoh
Cross River University of Technology, Nigeria

Felix Nti Koranteng
University of Education, Winneba, Kumasi Campus, Ghana

Joseph Ahor Abandoh-Sam
https://orcid.org/0000-0002-8815-0913
Valley View University, Ghana

ABSTRACT

Due to the sensitivity and amount of information stored on mobile devices, the need to protect these devices from unauthorized access has become imperative. Among the various mechanisms to manage access on mobile devices, this chapter focused on identifying research trends on biometric authentication schemes. The systematic literature review approach was adopted to guide future researches in the subject area. Consequently, seventeen selected articles from journals in three databases (IEEE, ACM digital library, and SpringerLink) were reviewed. Findings from the reviewed articles indicated that touch gestures are the predominant authentication technique used in mobile devices, particularly in android devices. Furthermore, mimic attacks were identified as the commonest attacks on biometric authentic schemes. While, robust authentication techniques such as dental occlusion, ECG (electrocardiogram), palmprints and knuckles were identified as newly implemented authentication techniques in mobile devices.

DOI: 10.4018/978-1-7998-3149-5.ch011

INTRODUCTION

In recent times mobile devices have gained popularity and have become an integral part of our daily lives. This popularity and rise is a result of the mobility and portability of computing devices in addition to its ability to store personal information that allows users to perform relevant tasks as and when required (Lee et al., 2016). However, the sensitivity and amount of information stored on mobile devices make it susceptible to vulnerabilities. Notably, there is a higher risk of breach in privacy due to ease of losing the device (Abdulaziz and Jugal, 2016). This has called for an increased need for improved authentication mechanisms in mobile devices. Mobile user authentication is the process of verifying and ensuring that only authentic and authorized users are granted access to the mobile device. It is achieved through assessing something the user knows (knowledge factor), something the user has (possession factor) and something the user is (biometric factor). Although the first two approaches contribute a great deal, they are faced with drawbacks that make them vulnerable to both internal and external attacks. Hence, it is an inefficient method for authentication (Shankar et al., 2016). The third has gained popularity as an authentic alternative to the first two categories (Tao and Veldhuis, 2010).

Biometrics authentication (i.e. "something the user is") is a unique, non-duplicable, non-transferable and automated recognition of individuals based on their physiological or behavioural characteristics (Saevanee et al., 2012). The use of biometrics as a means of authentication is convenient as users carry their biometrics identity always. Also, biometrics are reliable since they ensure the physical presence of users (Tao and Veldhuis, 2010). Furthermore, in mobile devices, it has an added advantage because no external hardware device or sensors are required for authentication. Modern mobile devices are developed and equipped with inbuilt sensors which can be used to achieve this task. Data extracted with these sensors are used for implicit user authentication as well as protection against unauthorized access to sensitive information (Crawford and Renaud, 2014). Despite the current increase in mobile biometric authentication research, literature on its progress, patterns and trends of implementation is lacking.

Accordingly, this chapter presents a systematic review of biometric authentication techniques used in mobile devices. It seeks to provide researchers and practitioners summaries of related issues on biometric authentications on mobile devices. The paper is presented as follows: firstly, literature on existing related systematic review studies is presented, this is followed by the motivation for the study, a list of review questions and the methodology used for conducting the review. The findings and results from the selected articles are summarized before discussions and conclusions are drawn.

RELATED STUDIES

To justify the need for this review, a search for existing systematic reviews on the subject area was conducted. The aim of this was to establish the current status of research summaries done in the subject area.

Guliani et al., (2018), Jagadeesh and Patil (2017) as well as Patil and Gudasalamani (2016) surveyed iris recognition system. In their review, they provided various methods and algorithms used by different researchers and their effect on the performance of iris recognition systems. They explained the evolution of various parameters to enhance the recognition ability of a biometric method and identified the drawbacks and future works. As a tool for electronic transaction authentication and electronic assessment Ojo et al., (2016) and Shunmugam & Selvakumar (2015) discussed uni-modal biometrics and its