Chapter 17
Comparative Analysis of Biometric Approaches in Continuous Authentication

S. Ayeswarya
https://orcid.org/0000-0002-2010-2579
Vellore Institute of Technology, India

John Singh
https://orcid.org/0000-0002-2674-488X
Vellore Institute of Technology, India

ABSTRACT

In an era where security and user authentication are paramount, continuous authentication methods have gained significant attention. This chapter aims to provide a comprehensive comparison of various biometric methods used for continuous user authentication. Biometric authentication techniques offer unique advantages in terms of security, usability, and continuous monitoring capabilities. This chapter will explore and evaluate different biometric modalities such as fingerprint, iris recognition, voice recognition, facial recognition, and behavioral biometrics. The comparative analysis will consider factors such as accuracy, reliability, cost-effectiveness, scalability, and user acceptance. Additionally, the chapter will discuss challenges, emerging trends, and future directions in the field of continuous user authentication using biometric methods.

DOI: 10.4018/979-8-3693-8014-7.ch017

INTRODUCTION

In the digital age, securing access to information and systems has become paramount. Traditional methods of authentication, such as passwords and PINs, are increasingly viewed as insufficient due to their susceptibility to theft, forgetfulness, and ease of breach (Ayeswarya & Singh, 2024). The advent of biometric authentication has revolutionized the security landscape by leveraging unique physiological and behavioral characteristics that are inherently difficult to replicate or steal. Biometric authentication traditionally involves verifying a user's identity at a single point in time, typically during login (Ayeswarya & Norman, 2019). While effective, this approach has limitations, particularly in scenarios where prolonged access to sensitive information or systems is required. This is where continuous authentication comes into play. Continuous authentication is an advanced security mechanism that continuously verifies a user's identity throughout the duration of a session, providing ongoing assurance that the person accessing the system remains the legitimate user. The primary objective of continuous authentication is to mitigate the risks associated with session hijacking and unauthorized access that can occur after initial login (Ayeswarya & Singh, 2024). By constantly monitoring and verifying the user's identity, continuous authentication ensures that even if an intruder gains access, their presence is quickly detected and countermeasures are deployed. This dynamic approach to security is especially critical in high-stakes environments such as banking, healthcare, and government systems, where the integrity and confidentiality of data are paramount. Continuous authentication can be implemented using various biometric modalities, each with its own set of advantages and challenges. The main biometric approaches include fingerprint recognition, facial recognition, voice recognition, iris recognition, and behavioral biometrics (Mondal, 2016). These methods vary in terms of accuracy, user convenience, susceptibility to spoofing, and privacy implications.

This chapter provides a comprehensive comparative analysis of these biometric approaches in the context of continuous authentication. By examining their mechanisms, strengths, and weaknesses, we aim to provide a clear understanding of how each modality performs in ensuring ongoing user verification. Furthermore, we will explore the potential for integrating multiple modalities to enhance security and usability, and discuss the future directions of continuous authentication in the evolving cybersecurity landscape. As we delve deeper into the specifics of each biometric approach, it becomes evident that the choice of modality is influenced by the particular requirements and constraints of the application at hand. Whether prioritizing accuracy, usability, security, or privacy, continuous authentication systems must strike a balance to effectively safeguard against unauthorized access while maintaining a positive user experience. In the subsequent sections, we will analyse