Chapter 3
Human Behavior–Based Keystroke Password Authentication:
A Behavioral Biometrics Approach

Arun Agrawal
https://orcid.org/0000-0001-7233-6660
Institute of Technology and Management, Gwalior, India

ABSTRACT

This article presents the development of a keystroke password authentication system based on the uniqueness of human typing behavior as behavioral biometrics. It analyzes keystroke dynamics, including timing, speed, and rhythm, providing a unique and secure method for user authentication. Traditional password-based systems are vulnerable to attacks such as phishing and brute force. Keystroke-based systems require the correct typing pattern along with the password, adding an extra security layer. This paper reviews existing methods, noting their strengths and limitations, and proposes a model using advanced machine learning algorithms to enhance accuracy and reliability. The proposed keystroke dynamics method demonstrates high accuracy and low false positive rates, proving its effectiveness in preventing unauthorized access. The results emphasize its potential as a reliable solution for secure authentication in modern network security frameworks.

1. INTRODUCTION

In today's world of digital transactions, the safety of personal and organizational information has become a top priority. Every online activity, from logging into an

DOI: 10.4018/979-8-3373-4972-5.ch003

email account to transferring funds, involves the exchange of sensitive data. Protecting this data is a constant challenge. Traditional methods like passwords, once seen as secure, are no longer enough to stop cyber threats. The scale of the problem is clear. In 2022 alone, over 24 billion passwords were reported as compromised. The situation is worse when weak passwords such as "123456" remain in common use despite years of awareness campaigns (Conklin et al., 2004).

Weak password practices continue to expose individuals and organizations to major risks. Studies show that 70% of basic web application attacks exploit poor credential management (Saadi et al., 2024). These numbers show how vulnerable current systems are. Passwords remain the most widely used authentication tool, yet they also serve as the weakest link. Many users rely on simple passwords or reuse them across multiple accounts. Such behavior makes it easier for attackers to guess or steal credentials. Once a single password is leaked, multiple accounts of the same user may become exposed. This creates a chain of security failures.

The growing number of attacks calls for new ways of securing digital identities. One approach is behavior-based authentication. This method goes beyond static credentials like passwords or PINs. It studies how users interact with devices and systems. Among the different forms of behavioral biometrics, keystroke dynamics has gained attention for its practicality and effectiveness (Bhardwaj & Gounder, 2020).

Keystroke dynamics is based on the observation that every individual has a unique typing style. Just like fingerprints or voice patterns, typing habits cannot be easily copied. These habits include the speed of pressing keys, the time taken between two key presses, and the pressure applied while typing. Over time, these patterns remain consistent for a user but differ greatly from one person to another. Cybersecurity experts consider this natural uniqueness a strong shield against impersonation (Sabaiter, 2019).

The strength of keystroke dynamics lies in its simplicity and its invisibility to the user. Unlike additional security tools that require hardware tokens or biometric scanners, keystroke dynamics works silently in the background. A user continues typing normally, while the system records and evaluates their patterns. If the typing style matches the stored profile, access is granted. If not, the system can deny entry or request additional verification. This extra step adds another barrier for attackers.

Even if an attacker somehow obtains a correct password, they still face the challenge of replicating the legitimate user's typing style. Mimicking keystrokes is extremely difficult. For instance, two users may type the same word but with different rhythms, pauses, and keypress durations. Such details are almost impossible to copy without being detected. This makes keystroke dynamics effective against credential stuffing and brute-force attempts.

The method also reduces reliance on strong passwords alone. Many users struggle with creating and remembering complex passwords. As a result, they prefer shorter