# Continuous online user authentication based on keystroke dynamics

**André Artelt[1,2,*], Jonathan Jakob[1,2,*], and Valerie Vaquet[1,2,*]**

[1]Faculty of Technology, Bielefeld University, Universitätsstraße 25, Bielefeld, Germany
[2]Corresponding mails: {aartelt, jjakob, vvaquet}@techfak.uni-bielefeld.de
*Authors are listed in alphabetical order

The growing market of internet services requires secure authentication methods. Particularly, new services need authentication over a longer period of time. For example, online universities need to make sure that the person taking an online examination is their actual student. Therefore, traditional login routines (username & password) are not sufficient for all use cases anymore.
One possibility to ensure continuous authentication is to apply biometric/behavioural patterns such as voice, handwriting, or keystroke dynamics. Since it is much harder to share or steal a person's traits or behavior, biometric authentication models are considered safer than traditional approaches [1].
In this contribution, we focus on keystroke dynamics. In particular, we attempt to continuously authenticate a user based on features such as *dwell time*, *flight time*, key down/up events, or times for certain bi- or trigrams [2].
The majority of the related work (see [1]) is only considering a short and fixed time window for authentication. Typically, a bunch of statistics on keystroke dynamics features like dwell/flight time is computed and classified.

We propose a *memory efficient method* for continuously authenticating users over time, based on their keystroke dynamics. We split time into small chunks (time windows) and classify each time window separately using common methods from literature [1, 2]. We integrate the classifications over time by using a *sequential bayesian hypothesis testing* framework. Therefore, we only have to store and process a small chunk of data at every point in time and can discard it afterwards.
Because of a lack of publicly available data sets for evaluation, we *created our own keystroke dynamics data set* which contains keystroke and mouse dynamics data from 32 subjects.

## References

[1] M. Karnan, M. Akila, and N. Krishnaraj. Biometric personal authentication using keystroke dynamics: A review. *Applied Soft Computing*, 11(2):1565–1573, 2011. issn: 1568-4946. doi: https://doi.org/10.1016/j.asoc.2010.08.003. url: http://www.sciencedirect.com/science/article/pii/S156849461000205X. The Impact of Soft Computing for the Progress of Artificial Intelligence.

[2] R. Moskovitch, C. Feher, A. Messerman, N. Kirschnick, T. Mustafic, A. Camtepe, B. Lohlein, U. Heister, S. Moller, L. Rokach, and Y. Elovici. Identity theft, computers and behavioral biometrics. In *2009 IEEE International Conference on Intelligence and Security Informatics*, pages 155–160, June 2009. doi: 10.1109/ISI.2009.5137288.