Journal of Human Development and Communication
Volume 15, Special Issue 2026 [133-142]

Typing Behavior in Web Authentication: A Human-Computer Interaction Case Study

Mohd Noorulfakhri Yaacob, Syed Zulkarnain Syed Idrus, Wan Nor Ashiqin Wan Ali

Fakulti Komputeran Cerdas, Universiti Malaysia Perlis

ABSTRACT

This research investigates keystroke dynamics as an interdisciplinary phenomenon from the perspective of human-computer interaction theory, viewing typing synchrony as an interactional episode between human and computer rather than as a singular biometric security tool. In the present study, 200 users were enrolled, each typing the same short phrase multiple times, and their patterns of movement rhythm and pauses were examined to better understand the human experience of behavioral authentication. Our analysis reveals that typing patterns are highly distinctive yet variable, reflecting complex interactions between motor learning, cognitive processing, and individual differences. We present an in-depth comparison of two contrasting cases that illustrate the design challenges: User 400 demonstrated fast, consistent typing with stable interkey intervals (100-150ms average) and minimal variability, suggesting well-developed motor automaticity. In contrast, User 380 exhibited slower, more variable typing (average 200-400ms) with pronounced cognitive pauses, particularly at word boundaries and capital letters (delays up to 1,296ms). Neither typing style is inherently superior; both represent legitimate human behavior patterns. These individual differences have critical implications for authentication system design. Generic one-size-fits-all models would either exclude variable users like User 380 through excessive false rejections or provide inadequate security for consistent users like User 400. Our findings demonstrate that behavioral authentication systems must employ personalized models, adaptive thresholds, and transparent feedback mechanisms to accommodate natural human diversity. Systems must treat variability as a normal characteristic of human behavior rather than a suspicious anomaly. This work challenges the prevailing paradigm that treats typing patterns as stable biometric templates, arguing instead for a user-entered design that embraces individual differences, ensures fairness across diverse populations, and respects user autonomy through transparency and control.

Keywords: Keystroke Dynamics, Behavioral Biometrics, Human Computer Interaction, User Experience, Typing Behavior, Individual Differences, Fairness, Accessibility .

1.0 INTRODUCTION

As digital platforms embrace more sensitive functionalities, the use of traditional security protocols, such as passwords, becomes less defensible. Analyzing how users' type, as opposed to what they type, adds the dimension of behavioral biometrics. From the perspective of keystroke dynamics, there are 3 temporal features of interest: the pace at which the individual types (i.e., typing speed), how long a key is held down (i.e., key hold duration), and the duration between keystrokes (i.e., interkey intervals). Given how unique and difficult to replicate such behaviors are, they are valuable for authentication and the ongoing detection of atypical system actions. Despite the potential of keystroke biometrics, most studies focus on algorithmic accuracy and the system's security attributes. The human factors involved in the system's practical usability, acceptability, and fairness seem insufficiently examined. This paper seeks to understand how and why people type, using a human-computer interaction (HCI) perspective, which regards typing as a biometric interaction between a user and a computer.

*Corresponding author: fakhri@unimap.edu.my

We analyzed the behavior of 200 subjects who were asked to complete the same typing task across several sessions. Rather than enforcing population-level accuracy measures that would standardize measures across all subjects, we explain individual accuracy measures to determine the extent to which subjects may have different behavioral profiles. We present two of the most extreme cases: User 400, a fast and accurate typist, and User 380, a typist who took her time and who experienced cognitive pauses during the exercise. While one typing behavior may be more desirable than the other in some situations, both are equally authentic. Our findings suggest that behavioral authentication has some fundamental challenges. When typing speed, typing accuracy, and typing consistency differs across a population, behavioral models that have been designed tend to be ineffective. If a system were designed to be highly flexible in its authentication behavior, accurate and fast typists like User 400 would be inappropriately classified as high-risk users. If only typists like User 380 were in use, the system's authentication behavior would be far too flexible. These challenges indicate that a balance between system security and usability must be struck. The best systems will use the complete system security/usability trade-off to personalize model behavior. This will be accomplished by dynamically adjusting authentication behavior thresholds and providing more transparent models to the user.

2.0 LITERATURE REVIEW

This section reviews prior studies on behavioral biometrics, keystroke dynamics, and human–computer interaction. It identifies key concepts, challenges, and research gaps relevant to user-centered authentication systems.

2.1 Behavioral Biometrics in HCI: Understanding the User Perspective

Instead of identifying users based on physical traits such as fingerprints, behavioral biometrics focuses on users' everyday interaction patterns such as typing rhythms, mouse movements, and touch gestures (Finnegan et al., 2024). Because it can use everyday devices and doesn't require specialized hardware, this method is very appealing for internet systems (Stragapede et al., 2022). That said, it does raise some HCI concerns, such as users collecting data unbeknownst to them, users not understanding what data is being collected, and users feeling more surveilled than protected (Baig et al., 2023). Among the many behavioral biometrics, keystroke dynamics is the most extensively studied. Initial studies showed that timing features such as keystroke hold times and inter-keystroke delay durations could accurately classify users at the individual level. That said, the performance of this method relies heavily on the quality of the data, and considerable user variability along with the design of the system. From an HCI perspective, it is not enough to be technically accurate. The systems also have to be understandable and acceptable to the users.

Studies on usable security have demonstrated that user acceptance is contingent on risk, context, and transparency, in that order. Users who have a grasp of the rationale behind data collection and the data obtained are more likely to welcome surveillance across behaviors (Reuter et al., 2022). User-centered design mandates an unambiguous explanation of the instances and reasons surrounding the collection of behavioral data, provision of control to users where practicable, along with transparency as to how the collected data is utilized for authentication(Ejaz et al., 2025). The systems also need to account for differences in users' typing skills and consistency, as applying a single model to all users will likely disenfranchise a subset of legitimate users who exhibit atypical behavioral patterns relative to the majority.

2.2 The Psychology of Typing: Motor Behavior and Cognition

One of the skills required to touch type is the ability to coordinate various elements involved in the action to achieve a successful outcome. When beginners start their typing journey, they tend to look for the keys and carefully select the one they need to press. Typing patterns are irreversible and reflect the typist's history. For example, self-taught typists and those with formal training often demonstrate varying timing patterns. Hand dominance can also affect the typing pattern displayed on a keyboard (Proctor et al., 2023). In addition to this, people often experience higher dominant hand timing asymmetry as they become more familiar with a keyboard, as keyboard switches can be a source of increased variability in typing to a point of muscle memory of the keyboard (Waes et al., 2021). These patterns that have developed throughout a typing career are often referred to as "fingerprints".

The motor activity of typing often reflects real-time cognition. If typing is paused, this can indicate that the typist is searching for a word/adequately planning a sentence, or making a decision (Alfalahi et al., 2022). If there are rapid bursts of typing, this suggests a highly practiced sequence and that the typist is likely composing. Context is very important for accurately authenticating typing. For example, if a phrase is to be transcribed quickly, the typing will likely occur in an automated rhythm. This shows the cognitive demand of typing, which, in turn, means that cognitive task demands need to be taken into account.

2.3 User Acceptance and Privacy Concerns in Biometric Systems

Legitimate biometric systems offer user-friendly solutions and eliminate the need to remember passwords. However, the extent to which users feel comfortable with such systems and how they perceive control are essential to their success. Systems employing behavioral biometrics face other concerns due to the continuous and stealthy nature of data collection, which further obstructs individuals' informed decision-making (Rukhiran et al., 2023).

Unfortunately, the users impacted by the systems have the least control. Even when data collection is conducted in a privacy context, users perceive it as abusive (Baig & Eskeland, 2022). As an example, users may accept keystroke dynamics for fraud detection while logging into a secure account, but may reject the practice during passive employee monitoring and behavioral and targeted advertising. Users place more emphasis on purpose and context than on the actual technology being employed. Users’ reluctance is also rooted in the permanence of data collection: users of a system can change passwords if they notice a compromise; however, they are unlikely to view biometric templates in the same light due to the permanent nature of their storage. Even when keystroke dynamics are used for timing rather than content, users will still perceive negative aspects of the system, such as unfair profiling, unjust surveillance, unwanted decision-making, and opacity (Stragapede et al., 2023).

Adopting privacy by design means building a system with protections baked in during the design phase, including active control over monitoring and, in the absence of biometrics, the option to choose a different form of authentication (S & K, 2025). The system is built in a fair manner with no user suffering harm from rejection due to biometric variability, and hence, will be fair to all users. The system should be fair across different users in terms of their typing style or ability and not disadvantage those users who’s typing patterns, on average, are different from those of the majority.

3.0 METHODOLOGY

This section outlines the research design, participant selection, data collection procedures, and ethical considerations employed in the study.

3.1 Research Design and Ethical Considerations

An analysis of mixed methods with computational and qualitative user experience. User experience longitudinal observational study wherein 200 participants completed several typing exercises in multiple (1-3) sessions. This within-subjects design enabled the study of individual typing patterns, their temporal stability, and contextual variability with respect to the task and time.

Approval of the study by the Institutional Review Board (IRB) was obtained for all procedures. Participant interaction was voluntary, and informed consent was obtained prior to data collection. It was explained to participants that the study focused on their typing behavior as a natural interaction, not as surveillance. It was particularly important that only the timing of the keystrokes was captured, and not the content that participants typed. This keystroke-timing-without-content approach was meant to alleviate privacy concerns while still enabling behavioral analysis. The data was anonymized, encrypted, and stored in a secure location accessible only to members of the research team. Participants had the right to withdraw at any time and request that the data be deleted.

3.2 Participant Recruitment and Demographics

To ensure a varying demographic condition while accounting for age, typing experience, native language, and physical ability, varying forms of purposive stratified sampling were performed, which included participants on university email distribution lists, community boards, and social media, where all participants, regardless of experience, were encouraged to be included. This was done to ensure a comprehensive collection of typing data, and not just for advanced users.

Recruiting participants used purposive sampling, which limited potential participants to those over 18, able to type independently (or with assistive devices, which was not an exclusion criterion) on a standard keyboard, and able to attend multiple sessions. 200 participants completed the study, including students, office workers, technical staff members, and a civilian population, all aged 18 to 65, resulting in a range of typing speeds. This included very slow, only using a hunt-and-peck method, to touch typing, and even using other assistive technologies, which may have been combined with a motor impairment, and even advanced. This range of demographics was vital to assess the fairness of typing-based authentication across diverse populations.

3.3 Data Collection: Creating a User-Centered Experience

Data collection environment took care to achieve an optimal level of balance between control, experimentation, rigour, and ecological validity. The space used for the study was quiet, had comfortable seating, and was free of time pressure. Researchers remained available to answer questions, but were unintrusive. Participants were provided with an internet-based app/interface designed with the principles of transparency and user ease. The interface gave instructions, indicated progress, and provided visual alerts to inform participants when their time was being recorded. Privacy reminders explained that only the timing mechanism's action was recorded.

Participants were able to type naturally at their own pace, making mistakes and using the backspace key to delete characters and correct errors. To capture real behaviors, as opposed to a false impression of accuracy, every keystroke and error were recorded. During the post-task debrief, participants were shown a simple visualization of their own keystroke data to help demystify data collection and monitoring. This took the form of the participant being presented with a visualization of their own typing pattern.

The participant's main activity in this study was to type the same phrase, "durian raja buah Malaysia," 7 times per session. This exercise was primarily to gauge the baseline timing trends for when the participant was under virtually no load in response to the question (to allow for consistent content across participants). The interface programmed in JS tracks keyboard entry and release events as kilobytes for their respective delay in real time to derive the keystroke features in milliseconds, for example, the time in which a key is held down, the time it takes for a key to be released, and the time it takes to press the next key.

This section presents and analyzes the study findings, with emphasis on individual typing patterns and variability among users.

3.1 Overview of Findings

This section details findings from our study. Two hundred participants each typed the same standardized phrase repeatedly. While most analyses concentrate on population-level accuracy metrics, we focus on individual case analyses to see what human differences authentication systems must account for. Here, we describe in detail User 400 and User 380 as two contrasting examples at opposite ends of the behavior spectrum, with respect to the diverse authentic and legitimate typing patterns they display. Our analyses show that, while individual typing patterns are consistent and distinctive, and thus would support behavioral authentication as a secure metric, there are still substantial differences with respect to other participants and the same individual at different periods in time. Inter- and intra- individual variability of this kind is to be expected. It is a reflection of the human differences likely to be present across the domains of motor learning, cognition, and typing fluency. The system design challenge lies in accommodating intra- and inter-user differences between variable users and consistent users, to be fair to variable users and not to provide a consistent user with an unwarranted low level of system security.

The phrase "durian raja buah Malaysia" was selected as the standard seed phrase because the content is a common sore point in Malaysian geography and, as a consequence, is likely known to every local Malaysian. The phrase is also a good representation of routine-level automated execution of the motor program for typing, incorporating an uppercase letter, a word boundary, and 4 common letters of the English alphabet. This phrase was typed by every participant in the study across multiple sessions and from memory 7 times per session.

3.2 Individual Typing Patterns: User 400

User 400 exhibited consistent typing behavior throughout all of the trials. Interkey delays per trial were consistent within the 100-200ms range, indicating that the user demonstrated typing at a consistent, although moderate, speed across the trials, with noticeable control of their rhythm. Multiple temporal signatures were demonstrated by the user across all attempts. The most notable were the peaks at the 'aj' and 'ja' transitions with delays around 350ms. These delays signify the hand having to lift and reposition. Alternatively, the user had valleys (faster transitions) at the 'du' and 'aspace' transitions, which are in the 235ms range, indicating the user is well-practiced and has an efficient motor chunk.

The first word that sprang to mind when describing User 400 was consistency. There were multiple attempts to align the timing lines, and consistently, the peaks and valleys aligned perfectly in both timing and feature magnitudes. This indicated high levels of motor control and, therefore, very low variability in the task. Regarding behavioral authentication, User 400 was the ideal subject. The patterns recorded were unique to a single user, and they exhibited high temporal stability, down to the minute, over the duration of the study. Any system designed to model this user would be operating on extremely narrow margins, resulting in almost no false rejections.

Even User 400 exhibited some variation, with some trials showing slightly longer pauses mid-word, demonstrating their own patterns of behavior. These deviations could take the form of typical motor behavior or represent momentary distractions. These systems need to be programmed with greater finesse to recognize these fluctuations as the standard behavior of a human rather than as statistical outliers. This illustrates a fundamental problem with HCI: -differentiating data-compromising micro patterns of behavioral deviations from the lack of malicious intent embedded in human behavior.

3.3 Individual Typing Patterns: User 380

The typing pattern of User 380 was recorded and found to be considerably different than the others being analyzed. For User 380, the interkey intervals showed an extraordinary range of 61.609 ms, with a lower average base typing speed and increased temporal variability, with an average range of 200 ms to 400 ms. This user exhibited behavioral patterns with large spikes: 1007 ms interkey intervals with the 'spacer' and 1296 ms with 'spaceM'. These interkey intervals can be attributed to cognitive pauses during which the user is deciding on the next word, scanning and searching for the required keys, and/or readjusting the shift key, which can throw off the user’s typing flow. There was a notable lack of automaticity associated with typing the capital lthe letters as evidenced by the longer-than-average pause on the capital letters.

Additionally, albeit smaller, spikes were exhibited at 'aj' (627 ms), 'ay' (667 ms), and 'spaceb' (476 ms) transitions. These spikes, unlike the regular peaks exhibited by User 400, were highly variable across different trials; sometimes they were rapid, and at other times they were slower. This typing behavior is best explained by greater cognitive processing and attentional control rather than by a high degree of motor execution. The user in this case may have been thinking about the letters that were to follow, perhaps scanning for the required keys, and/or may have experienced a distraction during one of the letter-typing transitions.

User 380's responses were also the most inconsistent across the different trials. When looking at the results from multiple attempts, the lines became very spread out. Each trial had different sequences of intervals. The positions of the peaks and valleys would shift, and the magnitude contrasts would vary widely. The latter part of the sequences, in particular, showed very high irregularity, indicating that the sequences' consistency decreased over time, likely due to fatigue, lack of attention, or increased cognitive load.

From an authentication standpoint, User 380 is a really difficult case. The high variability of their responses means that wider tolerance thresholds will need to be set to avoid false rejections; however, this makes the system less likely to capture real security breaches, leading to a trade-off between usability and security. User 380 likely experiences more authentication friction than User 400, despite both being legitimate users, raising fairness concerns.

3.4 Identifying Individual Differences

The contrast between User 400 and User 380 is a great illustration of the spectrum of human typing behavior. There are four main differences:

Temporal Dynamics Scale: User 400 has a 2352ms range of the interval, while user 380 has a 61,609ms range, with a five-fold difference in max intervals. There is a considerable difference in average typing speed. User 400 has an average of ms 120 per keystroke, equivalent to 5060 WPM, while User 380 has an average of 350ms per keystroke, equivalent to 2535 WPM. There needs to be some accommodations for this range of speed for the systems in place so as not to be discriminatory for slower typers.

Peak Latencies: There is no response during the transition for both users, but the reasons are different for each user. The reason for user 400 is the largest peak, which is the letter combination and repositioning that needs to be repositioned for a motor constraint of 'ja' (352ms). For user 380, the reason for the letters is cognitive pauses at word boundaries and the use of capital letters rather than motor limits. The letters that peak are 'spacer(1,007ms)' and 'spaceM' (1,296ms). The reasoning for these characters is distinctive and allows for the creation of patterns, but due to the need for personalization, this cannot be done with a population average.

Pattern Repeatability: There is a significant difference in repeatability between user 400 and user 380. User 400 has high repeatability and lower variation, while user 380 has lower repeatability and higher variation. There is a strong chance that this within-person variability is the root cause of the system at hand being unreliable. The system for user 400 has learned a small profile with high predictability. The system for user 380 needs to be within a larger behavioral range for the profile to be described as loose. The need for modeling, as described, is the reason for the word "equitable" in the final sentence.

Baseline Typing Speed: User 400 was approximately twice as fast as User 380. Generally, the typing proficiency of an individual is an indicator of their expertise and/or the amount of training they have received. Touch typists show faster and more consistent patterns, as compared to hunt and peck typists. That said, speed alone should not be the basis for determining successful authentication as slower typists should have the same level of security as faster typists, plus the same level of usability. The key differences summarized in Table 1 are detailed with timing data in Table 2 in relation to the pairs of adjacent keys.

Table 1 Typing Characteristics Comparison

Metric	User 400 (Attempt 1)	User 380 (Attempt 1)
Phrase Typed	durian raja buah Malaysia	durian raja buah Malaysia
Total Typing Duration	~4,931 ms	~10,226 ms
Average Inter-Key Interval	100–150 ms	200–400 ms
Baseline Speed	Fast (moderate)	Slow (variable)
IKI Range (Min–Max)	2–352 ms	6–1,609 ms
Pattern Consistency	High (stable)	Low (variable)
Notable Peak Transitions	a-j (352 ms)	space-r (1,007 ms), space-M (1,296 ms)
Notable Valley Transitions	a-space (2 ms), d-u (35 ms)	a-h (6 ms), a-n (91 ms)
Typing Profile	Consistent, practiced	Variable, cognitive load

These comparisons demonstrate that behavioral authentication cannot rely on generic models. User 400 and User 380 both have legitimate typing patterns, yet their profiles differ fundamentally. Generic systems optimized for consistent users would unfairly reject variable users through excessive false rejections. Systems that accommodate high variability would sacrifice security for the sake of consistent users. Resolving this tension requires personalized modeling, adaptive thresholds, and transparent feedback design principles that we discuss in Chapter 5.

Table 3 Keypair Transition Timing Comparison

Key Pair	User 400 IKI (ms)	User 380 IKI (ms)	Difference	Observation
du	35	141	4.0×	User 400 very fast, User 380 moderate
ia	160	576	3.6×	User 380 major pause (peak)
spacer	243	1,007	4.1×	User 380 extreme pause (peak)
aj	13	627	48.2×	Dramatic difference! (peak)
ja	352	68	0.2×	User 400 peak, User 380 fast
aspace	2	61	30.5×	User 400 extremely fast (valley)
spaceM	170	1,296	7.6×	Capital letter: User 380 struggles
ay	153	667	4.4×	User 380 long pause (peak)

This section interprets the results in relation to human behavior, system design, usability, and fairness in behavioral authentication.

4.1 Understanding Typing as Human Behavior

This research suggests that keystroke actions reflect a range of human attributes, including, but not limited to, the mechanics of action. It encompasses the functions of the motor component, cognition, the typist's individuality, and other situational factors. Differentiating Users 400 and 380 typifies this range: User 400 engaged in fast, steady, and consistent keystroke activity, while User 380 did not, exhibiting slower, more erratic keystroke patterns.

This range of behaviors on the typing interface is a conundrum within the HCI framework. It isn’t congruent to simply state that behavioral patterns, in this case, keystroke actions, form a strong basis for authentication, as apparently, the behavioral patterns do not require special security devices, nor do they require integration of a behavioral password. These patterns, however, are not representative of a behavioral biometric template. They adapt relative to user context, level of exhaustion, degree of focus, and/or experience. Systems should account for variation of the human condition in a manner that is not dismissive. The typing behaviors of Users 400 and 380 are part of a continuum, with User 400 demonstrating far less variability than User 380. Systems should not focus on user groups consisting of a small proportion of the population to the exclusion of the rest.

4.2 Considerations for Designing Authentication Systems

The results from our research also contribute meaningfully to system design. Firstly, systems should implement individualized models rather than population-based template systems. Users 400 and 380 exhibit completely disparate behavior. Generic models will fail for both users. Each will require an individualized behavioral profile that captures and distinguishes between patterns and variance in behavior. Customization requires an enrollment phase in which the system learns the user’s normal behavior; however, this phase should not be overly burdensome. Our study involved five attempts, which took mere minutes to complete. The second parameter for system design should be that systems should also permit changes to the models over time. As users accrue experience, switch devices, or are in varied states physically the behavior underlying their typing will shift. Because initial models will become less effective over time, systems should revise user models in real time to reflect behavioral changes resulting from sustained authentication.

Thirdly, systems should calibrate individual user models and their tolerances. User 400 can be modeled with narrow tolerances due to their high consistency, while User 380 requires wider tolerances due to greater behavioral variability. When adjusting tolerances, there needs to be a sensible trade-off between the user experience, which is the system's primary purpose, and the risk of false rejections due to high variability and spontaneous behavioral changes. Each false rejection leads to end-user friction and frustration with the system which may ultimately lead to abandonment.

4.3 Fairness and Accessibility

Any ethical analysis regarding our comparisons must consider the fairness issues raised by our analysis. Is it fair that User 380 experiences more false rejections than User 400 because of the benign variability we've described? Failure to treat variability equitably may lead to discriminatory outcomes if it is related to protected attributes such as age, disability, or low income. In the realm of behavioral authentication, fairness requires that we measure and disclose the authentication error rates for each demographic segment. If such gaps are found, they must be closed, the behavioral models modified to address them, or the thresholds adjusted.

The deployed systems must offer the same level of security if they impose the same level of burden. User 380 should not have to endure additional friction in the authentication process simply because the User lacks Natural Typing Variability. If wider tolerance thresholds become the norm, systems must offset that by other means, perhaps by more heavily relying on other behavioral features or integrating keystroke dynamics with more secure (i.e. static) biometrics. Systems must also be accessible by design. Users with motor impairments, as well as those who may need assistive technologies, should be able to use the behavioral biometric authentication process. Design might also need to include additional input methods, different authentication models, or even the elimination of features that assistive technologies would affect. Finally, systems must allow opt-out and offer alternative authentication to those who are unable or unwilling to accept behavioral monitoring, enabling individuals to exercise autonomy and preventing exclusion.

This paper considered typing behavior not solely as a security mechanism but as an interaction between humans and their computers. Using a sample of 200 participants who repeatedly typed the same standardized phrase, we showed that typing behavior is influenced not only by biometric signatures but also by motor pattern learning, cognition, and individual traits. Our user sample is also a comparative study of extremes: user 400, who typed rapidly and consistently, vs user 380, who typed slowly and with high variability. This stands as an example of the core problem that users of a behavioral authentication system pose: both in this example, typists incorporated behaviors that were valid and authentic, and the system must make room for such variability.

Such results show that behavioral authentication systems are built on the assumption that typists are homogeneous. The systems in the study must operate on the assumption that all users will behave in a uniform way, with a limited set of characteristics detectable by the system. Authentication systems that assume behavioral uniformity will be highly dysfunctional. To counterbalance the assumption of behavioral uniformity, we propose integrating user-adaptive systems and feedback-based behavioral systems that can respond transparently to human diversity without penalty.

ACKNOWLEDGMENT

We would like to thank the Ministry of Higher Education for funding this research and supporting our participation in this conference through the FRGS/1/2024/ICT07/UNIMAP/02/3 grant (MyGrant).

REFERENCES

Alfalahi, H., Khandoker, A., Chowdhury, N., Iakovakis, D., Dias, S., Chaudhuri, K., & Hadjileontiadis, L. (2022). Diagnostic accuracy of keystroke dynamics as digital biomarkers for fine motor decline in neuropsychiatric disorders: a systematic review and meta-analysis. *Scientific Reports*, *12*. https://doi.org/10.1038/s41598-022-11865-7

Baig, A. F., & Eskeland, S. (2022). A Generic Privacy-preserving Protocol for Keystroke Dynamics-based Continuous Authentication. 491–498. https://doi.org/10.5220/0011141400003283

Baig, A. F., Eskeland, S., & Yang, B. (2023). Privacy-preserving continuous authentication using behavioral biometrics. *International Journal of Information Security*, *22*, 1833–1847. https://doi.org/10.1007/s10207-023-00721-y

Ejaz, U., Panchal, P. B., Islam, S., & Imashev, A. (2025). Behaviour Biometrics Using AI for Continuous Authentication Systems. *Journal of Artificial Intelligence General science (JAIGS) ISSN:3006-4023*. https://doi.org/10.60087/jaigs.v8i02.386

Finnegan, O., White, J., Armstrong, B., Adams, E., Burkart, S., Beets, M., Nelakuditi, S., Willis, E., Von Klinggraeff, L., Parker, H., Bastyr, M., Zhu, X., Zhong, Z., & Weaver, R. (2024). The utility of behavioral biometrics in user authentication and demographic characteristic detection: a scoping review. *Systematic Reviews*, *13*. https://doi.org/10.1186/s13643-024-02451-1

Proctor, R., Zhong, Q., & Chen, J. (2023). The Simon Effect Asymmetry for Left- and Right-Dominant Persons. *Journal of Cognition*, *6*. https://doi.org/10.5334/joc.265

Reuter, C., Iacono, L., & Benlian, A. (2022). A quarter century of usable security and privacy research: transparency, tailorability, and the road ahead. *Behaviour & Information Technology*, *41*, 2035–2048. https://doi.org/10.1080/0144929x.2022.2080908

Rukhiran, M., Wong-In, S., & Netinant, P. (2023). User Acceptance Factors Related to Biometric Recognition Technologies of Examination Attendance in Higher Education: TAM Model. *Sustainability*. https://doi.org/10.3390/su15043092

S, A., & K, J. (2025). Enhancing security and usability with context aware multi-biometric fusion for continuous user authentication. *Scientific Reports*, *15*. https://doi.org/10.1038/s41598-025-14833-z

Stragapede, G., Vera-Rodríguez, R., Tolosana, R., Morales, A., Acien, A., & Lan, G. L. (2022). Mobile Behavioral Biometrics for Passive Authentication. *Pattern Recognit. Lett.*, *157*, 35–41. https://doi.org/10.48550/arxiv.2203.07300

Stragapede, G., Vera-Rodríguez, R., Tolosana, R., Morales, A., Damer, N., Fiérrez, J., & Ortega-Garcia, J. (2023). Keystroke Verification Challenge (KVC): Biometric and Fairness Benchmark Evaluation. *IEEE Access*, *12*, 1102–1116. https://doi.org/10.1109/access.2023.3345452

Waes, L., Leijten, M., Roeser, J., Olive, T., & Grabowski, J. (2021). Measuring and Assessing Typing Skills in Writing Research. *Journal of Writing Research*. https://doi.org/10.17239/jowr-2021.13.01.04