JOURNAL OF
EMERGING INVESTIGATORS

Article

OTGP: An innovative biometric authentication system with on-the-go passwords using a novel typing signature

Shlok Shirodkar[1], Sankar Balasubramanian[2]
[1] Singapore International School, Mumbai, India
[2] Indian Institute of Science, Bangalore, India

SUMMARY

Traditional password systems are vulnerable to cyberattacks such as brute force and phishing attacks, while existing biometric methods like fingerprint and facial recognition require specialized hardware and can be compromised. Keystroke dynamics offers a promising alternative by analyzing unique typing patterns using standard keyboards without additional equipment, leveraging motor memory that is difficult for attackers to replicate. We hypothesized that typing patterns are unique to every individual and can serve as a reliable biometric authentication method. To test this, we developed specialized hardware using piezoelectric sensors integrated into a conventional keyboard, along with custom software that captures five typing parameters: typing speed, inter-key intervals, typing accuracy, keystroke duration, and keypress force. These parameters generate what we term a "typing signature" for each user. Our method enables On-The-Go Passwords—phrases dynamically created by users at their discretion. We conducted an experimental study with 30 participants from various demographic backgrounds across six sessions each to evaluate consistency, uniqueness, and reliability. Statistical analysis confirmed our hypothesis: typing signatures showed high consistency within individuals (mean Coefficient of Variation < 15%), clear distinctiveness between individuals (99.8% of pairwise comparisons showed significant separation), and significant age correlations for temporal and force metrics ($p < 0.05$), while maintaining discriminative power across demographic groups. These findings suggest typing signatures can serve as an effective biometric authentication method with practical applications in finance and healthcare.

INTRODUCTION

Protection of sensitive data and assurance of safe access to online platforms are critical due to the increasing rate and complexity of cyberattacks (1,2). While technology has rapidly advanced in fields like artificial intelligence (AI), passwords have not seen significant innovation with limited development having been documented over the last decade (3). Recently, there have been numerous incidents in which users have lodged complaints about falling prey to cyberattacks. The most common loss a user faces is mostly in the form of financial loss and identity theft, which results in mental tension and even depression at times (4,5). This is because conventional systems are prone to attacks like phishing, brute force attacks, and the danger of password reuse (6,7). These issues necessitate the search for a more secure and trustworthy authentication method that can operate smoothly across many environments.

Biometric authentication is a promising replacement for traditional password systems. It presents distinctive biological attributes and/or behavioural characteristics of a person to authenticate identities, thus giving an additional layer of security. The commonly employed biometric technologies are fingerprint scanning, facial scanning, and voice pattern recognition. These technologies are widely used in high-security domains like banking and mobile technology due to the ease with which they can accomplish a quick and precise identification (8). However, they are likely to require specialized technology for capture and analysis of individuals' physical characteristics, which imposes limits on accessibility, scalability, and adoptability (9). The features employed by these systems have been compromised by malicious actors due to recent technological advances (10).

To solve this problem, keystroke dynamics provides a fresh approach to behavioural biometrics by analyzing users' typing patterns (11,12). The field of keystroke dynamics, also referred to as typing biometrics, has been extensively researched as a behavioural biometric authentication method (13–19). Numerous studies have been carried out by researchers to demonstrate the efficacy of keystroke dynamics as an electronic fingerprint in several contexts (20,21). Keystroke dynamics are based on behaviour patterns of individuals that require a continuous flow of data, unlike a static biometric system that uses immutable physical attributes of an individual (1). The advantage of using keystroke dynamics is its ability to provide high security using temporal variations in typing patterns without the need for any specialized hardware (2). Researchers have employed machine learning and deep learning algorithms from the domain of AI to learn and authenticate typing patterns of individuals (22,23). It has been shown that keystroke dynamics remain effective in situations where traditional biometric systems based on physical attributes may be compromised (24). Another unique advantage of keystroke dynamics is its ability to accommodate a wide range of users, including people with certain disabilities, such as Parkinson's Disease, hand tremors, sclerosis, and dystonia. (25,26). The behavioural traits of the users during their regular keyboard usage are unique and provide a cheap and easily available substitute that helps to integrate these systems into the current digital systems (27,28). It provides the ability to improve the security features with no additional investment for any extensive upgrades or extra hardware (29).

Since typing is a skill acquired over a period of time and is set in the muscle memory of each individual, it becomes difficult for perpetrators to copy it at their will, either knowingly or even unknowingly, from the concerned user. The aim of this

https://doi.org/10.59720/25-052

research, therefore, is to establish these typing signatures as an authentic and unique identifier of individuals, thereby enhancing current authentication mechanisms to the next generation. We hypothesized that typing patterns are unique to every individual and can serve as a reliable biometric authentication method. To test this hypothesis, we evaluated the following criteria: (1) The typing signature is consistent for an individual—typing signatures remain consistent over time, despite natural variations that may occur due to muscle fatigue and/or emotional states; (2) the typing signature is distinct for each individual—typing signatures are unique to each individual, influenced by their neuromotor coordination, established muscle memory patterns, and habitual keystroke behaviours; and (3) typing signatures maintain their discriminative power across demographic groups—the system can reliably distinguish between individuals regardless of age or gender effects on typing patterns. In order to investigate the utility of a biometric authentication-based system, we present a biometric authentication method based on keystroke dynamics of an individual, which we refer to as the typing signature. We considered five different typing metrics (parameters) such as typing speed, inter-key intervals, typing accuracy, keystroke duration, and typing force. We built specialized hardware using piezoelectric sensors that were placed inside conventional keyboards, along with custom-built software for recording these typing parameters. We used sophisticated algorithms to analyze the data to create the biometric typing profile of an individual. We conducted experimental studies to evaluate the intra-user consistency and inter-user distinctiveness of typing patterns. The data collected as part of the study showed that the individual's typing habit is distinctive and resistant to illegal copying. The results showed that typing signatures consistently exhibited strong characteristics of distinctness suitable for user differentiation and authentication. The findings suggest that this method can be used as an effective alternative to current security systems. This can help to build an inclusive digital security system for a wide range of users.

RESULTS

To investigate keystroke dynamics as a biometric authentication method, we developed a comprehensive data collection system combining specialized hardware with custom software applications. Our experimental setup utilized a modified keyboard equipped with piezoelectric sensors strategically positioned beneath each key to capture the precise force applied during typing, as demonstrated in our hardware configuration (**Figure 1**). We developed a complementary

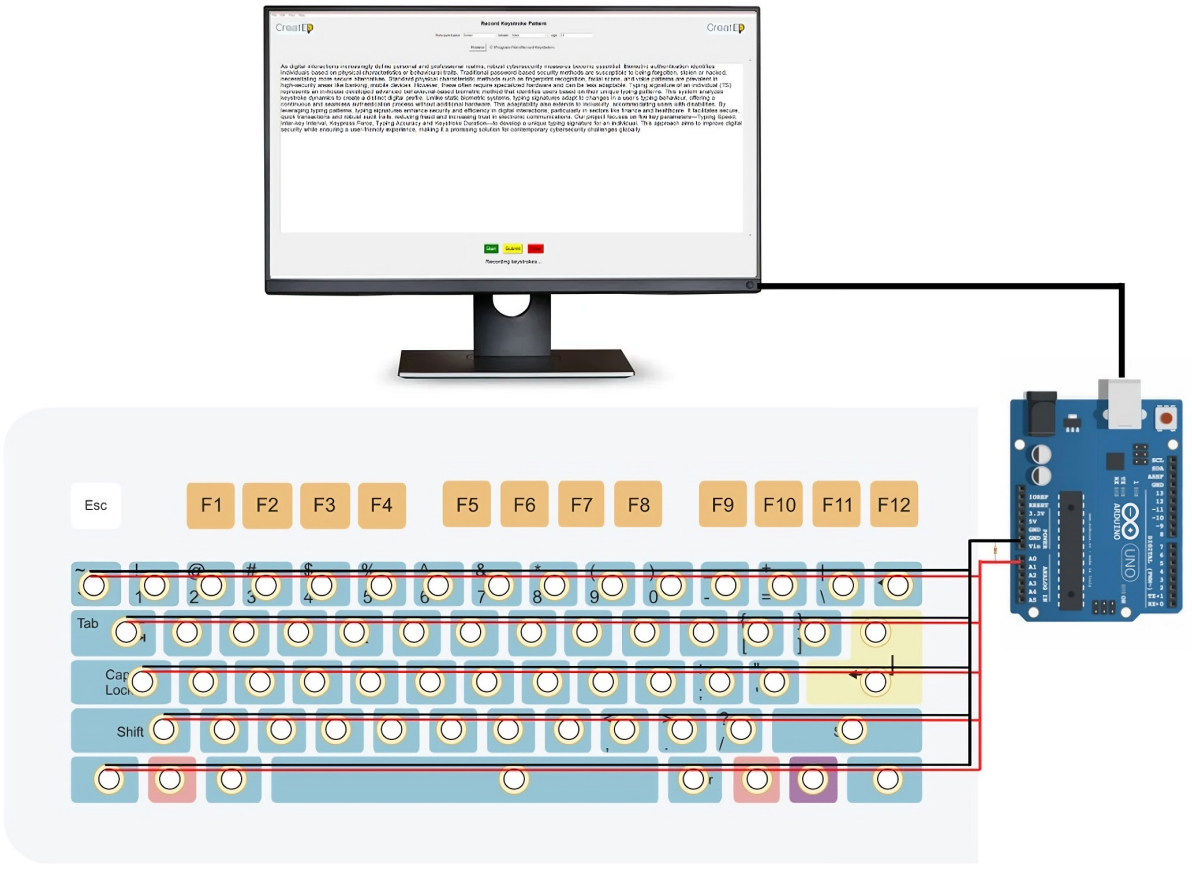


Figure 1. Hardware setup. System architecture showing the custom keyboard with integrated piezoelectric sensors, Arduino Uno microcontroller, and computer interface. The piezoelectric sensors, shown as circular elements, are placed beneath each key to measure keypress force. The sensors are connected in a grid formation to the Arduino Uno, which processes the analog signals and transmits digital data via USB connection to the computer. The monitor displays the custom software interface for data collection and real-time visualization of typing parameters.

https://doi.org/10.59720/25-052

Python-based software application to simultaneously record additional typing metrics, including speed, inter-key intervals, accuracy, and keystroke duration, providing a complete digital interface for comprehensive data capture. We collected data from 30 participants over 6 sessions each (separated by 2-3 days), with participants typing a standardized pangram text designed to elicit natural typing patterns across all keyboard keys. We plotted the parameters of keystroke dynamics as measured for one participant (**Figure 2**).

Consistency of typing signature

To evaluate the consistency of typing signatures, we examined typing metrics for all participants across different sessions. We generated a spider plot to show how individual typing signatures changed over six sessions. The results showed that there were no noticeable differences between sessions, indicating that the participants' typing habits remained constant over time, with a standard deviation of ±1% (**Figure 3**). Intra-participant standard deviations for temporal

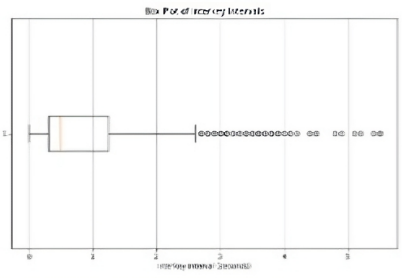
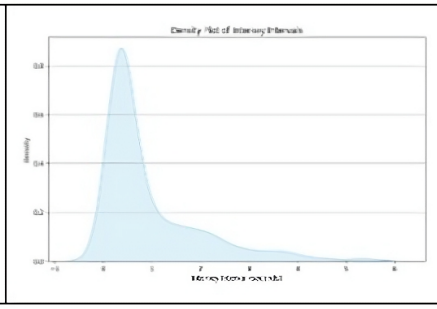
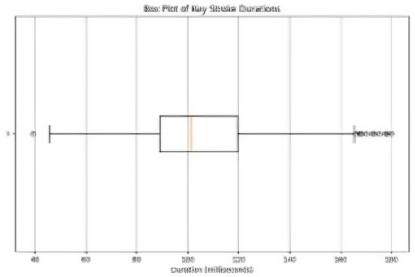
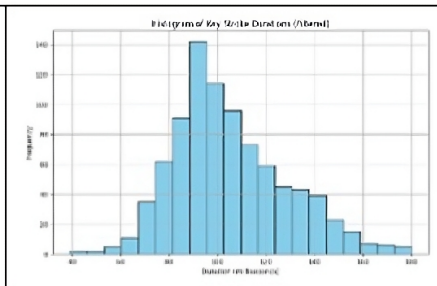
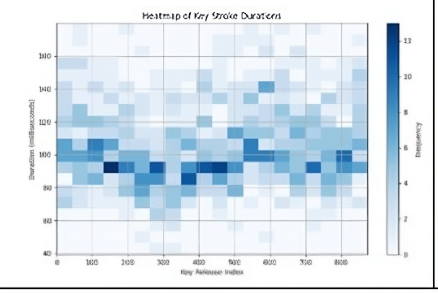
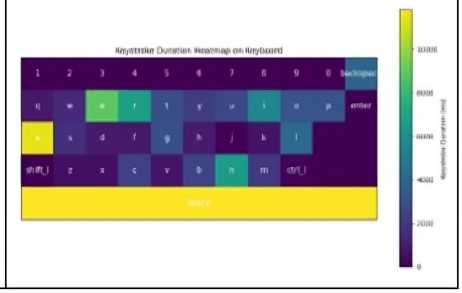
Typing Speed (TS)	55.14 CPM	
Typing Accuracy (TA)	78.38 %	
Keypress Force (KPF)	30.35 cN	
Interkey Interval (IKI)	Mean: 936.2 ms	
	Standard Deviation: 1002.4 ms	
		
Keystroke Duration (KSD)	Mean: 105.13 ms	
	Standard Deviation: 23.31 ms	
		
Keyboard Heatmap (KHM)		

Figure 2. Parameters of keystroke dynamics measured for one participant (P1). (a) Inter-key Interval (IKI) distribution with box plot showing median, quartiles, and outliers (left) and density plot showing normal distribution with mean of 936.2 ms and standard deviation of 1002.4 ms (right). (b) Keystroke Duration (KSD) distribution with box plot displaying statistical spread (left) and histogram showing frequency distribution with normal curve overlay, mean of 105.13 ms and standard deviation of 23.31 ms (right). (c) Keyboard heatmaps showing keystroke frequency distribution across the keyboard layout (left) and keypress force intensity map where warmer colors indicate higher force application in centiNewtons (right).

https://doi.org/10.59720/25-052

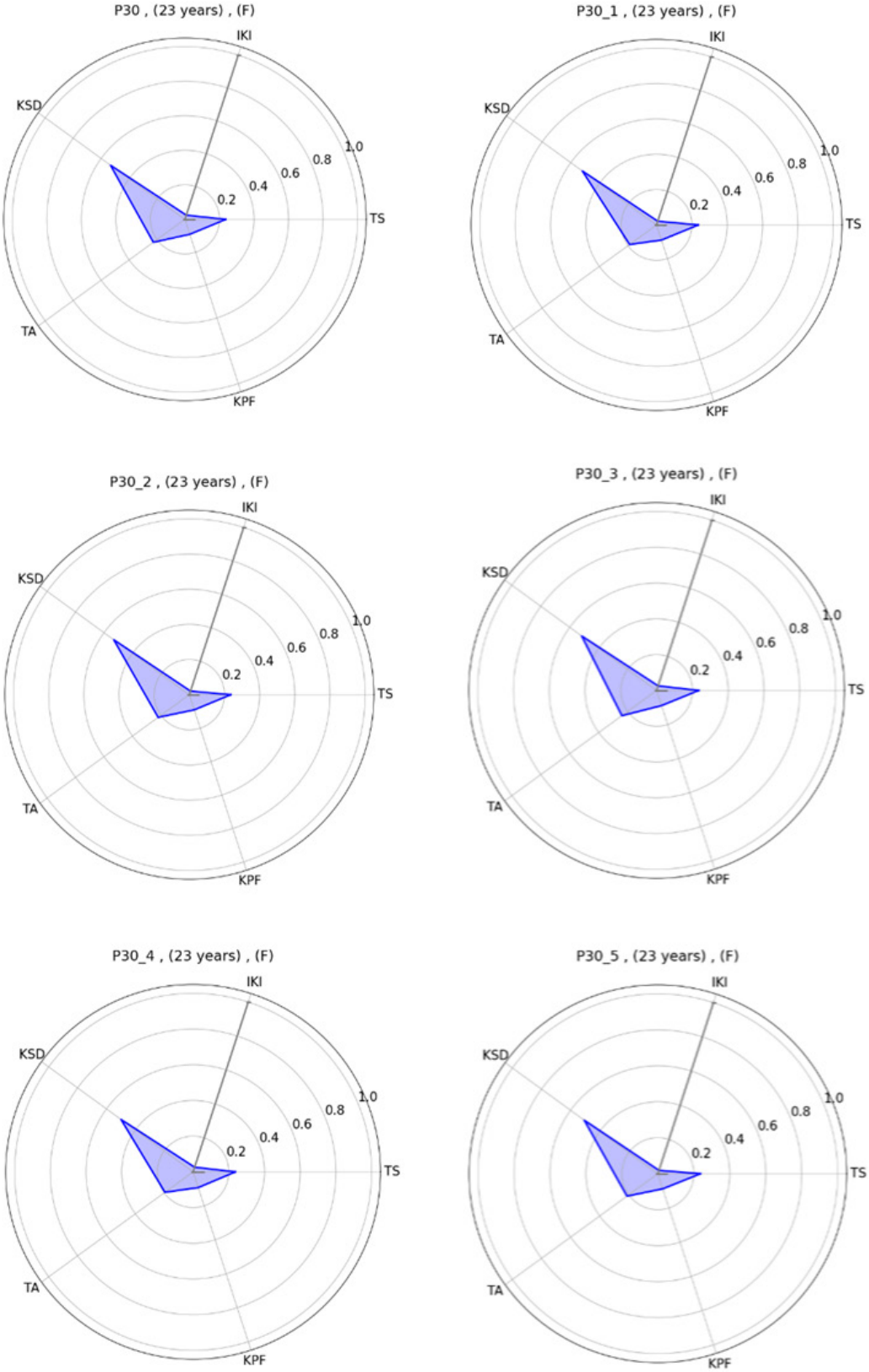


Figure 3. Typing signature of one participant (P1) across six sessions. The images show six typing signatures of the same individual generated during different sessions.

https://doi.org/10.59720/25-052

metrics averaged less than 15% of their respective means. For example, Participant 1 (P1) had a mean typing speed of 55.14 characters per minute (CPM) and a standard deviation of 1.32 CPM across several trials. The time between keys also changed very little, by less than 3%.

Uniqueness of typing signature

To assess the uniqueness of typing signatures, we created a spider plot depicting the typing traits of all 30 participants (**Figure 4**). The typing signature of every person is defined by factors such as typing speed, inter-key interval, keypress force, and keystroke duration. We determined clear delineation and minimal overlap among typing signatures. The overall patterns across all participants demonstrate inter-individual variation, supporting our second prediction.

Reliability of typing signature

We evaluated the effectiveness of using typing signatures for biometric authentication by considering changes in typing metrics based on age and gender. We observed similar trends in typing speed and the time between key presses across different age groups (**Figure 5**). We found that younger people typically typed faster and had shorter intervals between key presses. It was observed that there are very small differences in typing metrics between genders (**Figure 6**). Consistent patterns were observed within demographic groups, demonstrating the system's adaptability to typical typing behavior changes and its potential reliability as a biometric tool. The incorporation of keypress force as a measurement parameter enhanced the system's capacity for individual trait recognition, facilitating accurate authentication across diverse user groups.

Statistical analysis using Pearson correlation and t-tests revealed significant age-related patterns. Age showed significant positive correlations with inter-key interval (IKI) ($r = 0.443$, $t(28) = 2.61$, $p < 0.05$), keystroke duration (KSD) ($r = 0.559$, $t(28) = 3.56$, $p < 0.05$), and keypress force (KPF) ($r = 0.656$, $t(28) = 4.59$, $p < 0.05$). These correlations indicate that older participants exhibited longer inter-key intervals, longer keystroke durations, and higher keypress forces. Typing speed and accuracy showed negative correlations with age but were not statistically significant ($p > 0.05$).

Gender-based analysis using independent samples t-tests revealed no statistically significant differences between males and females for any typing parameter (all $p > 0.05$). Specifically: TS ($t(28) = 0.612$, $p > 0.05$), IKI ($t(28) = 0.113$, $p > 0.05$), KSD ($t(28) = -1.082$, $p > 0.05$), TA ($t(28) = -0.961$, $p > 0.05$), and KPF ($t(28) = -0.929$, $p > 0.05$).

We performed comprehensive statistical analyses to validate our predictions. All statistical tests were conducted with an $\alpha = 0.05$ significance level. We analyzed within-participant variability using the coefficient of variation (CV) for temporal metrics. The mean CV for inter-key intervals was 9.76% (max: 14.71%), and for keystroke duration was 24.07% (max: 44.19%). These low CV values indicate high consistency, with 86.7% of participants (26/30) showing CV < 15% for IKI and CV < 30% for KSD, supporting H1 that typing signatures remain consistent ($p < 0.05$).

Distinctiveness of typing signature

To quantitatively assess the distinctiveness of typing signatures, we computed pairwise Euclidean distances between all participants using normalized features (z-score normalization). Among 435 pairwise comparisons, the mean distance was 2.96 (SD = 1.42), with a minimum distance of 0.40 and a maximum of 8.84. Only 1 pair (0.2%) showed a distance < 0.5, indicating that 99.8% of participant pairs were clearly distinguishable. The distribution of distances showed a normal-like pattern centered around 2.8–3.0, confirming that typing signatures are statistically distinct between individuals (**Figure 7**).

Demographic robustness analysis

We examined whether the distinctiveness of typing signatures persists across demographic subgroups. We divided participants into age groups (< 30, 30–50, > 50 years) and computed pairwise distances within each group. The mean distances remained consistently high across age groups (2.85, 2.91, and 3.02, respectively), with no significant difference (ANOVA, $F(2,27) = 0.432$, $p > 0.05$). Similarly, within-gender pairwise distances (male-male: 2.88, female-female: 2.94) were comparable to between-gender distances (2.91).

DISCUSSION

This study investigated whether typing signatures can serve as a reliable biometric authentication method. We hypothesized that typing patterns are unique to every individual and can be used for secure identification. To test this, we developed specialized hardware with piezoelectric sensors integrated into a conventional keyboard and custom software to capture five typing parameters: typing speed, inter-key intervals, typing accuracy, keystroke duration, and keypress force. We collected data from 30 participants across six sessions each and evaluated consistency, uniqueness, and reliability of typing signatures. Our results confirmed the hypothesis: typing signatures showed high intra-individual consistency (mean CV < 15% for temporal metrics), clear inter-individual distinctiveness (99.8% of pairwise comparisons showed significant separation), and maintained discriminative power across demographic groups. These findings demonstrate that typing signatures can serve as an effective biometric authentication method.

The consistent typing patterns observed across multiple sessions can be explained by inherent regularities in motor memory that remain stable under similar conditions over time. Small differences in typing speed, inter-key intervals, and keystroke durations can be attributed to transient variables such as fatigue or emotional state. However, these variations scarcely confounded the typing signature, which remained largely consistent across sessions. This consistency is essential for this technique to be reliably used as a behavioural biometric system.

The low overlap observed between typing signatures of different individuals provides evidence of their uniqueness. This uniqueness likely arises from individual differences in motor coordination and muscle memory. Typing is a complex coordination of cognitive and physical abilities, involving finger movements, hand-eye coordination, and acquired typing habits. These are influenced by an individual's physiological and psychological characteristics, such as hand morphology, typing experience, and preferred typing postures. Additionally, the use of multiple typing metrics enables the detection of minute differences in typing behaviour, thereby creating a

https://doi.org/10.59720/25-052

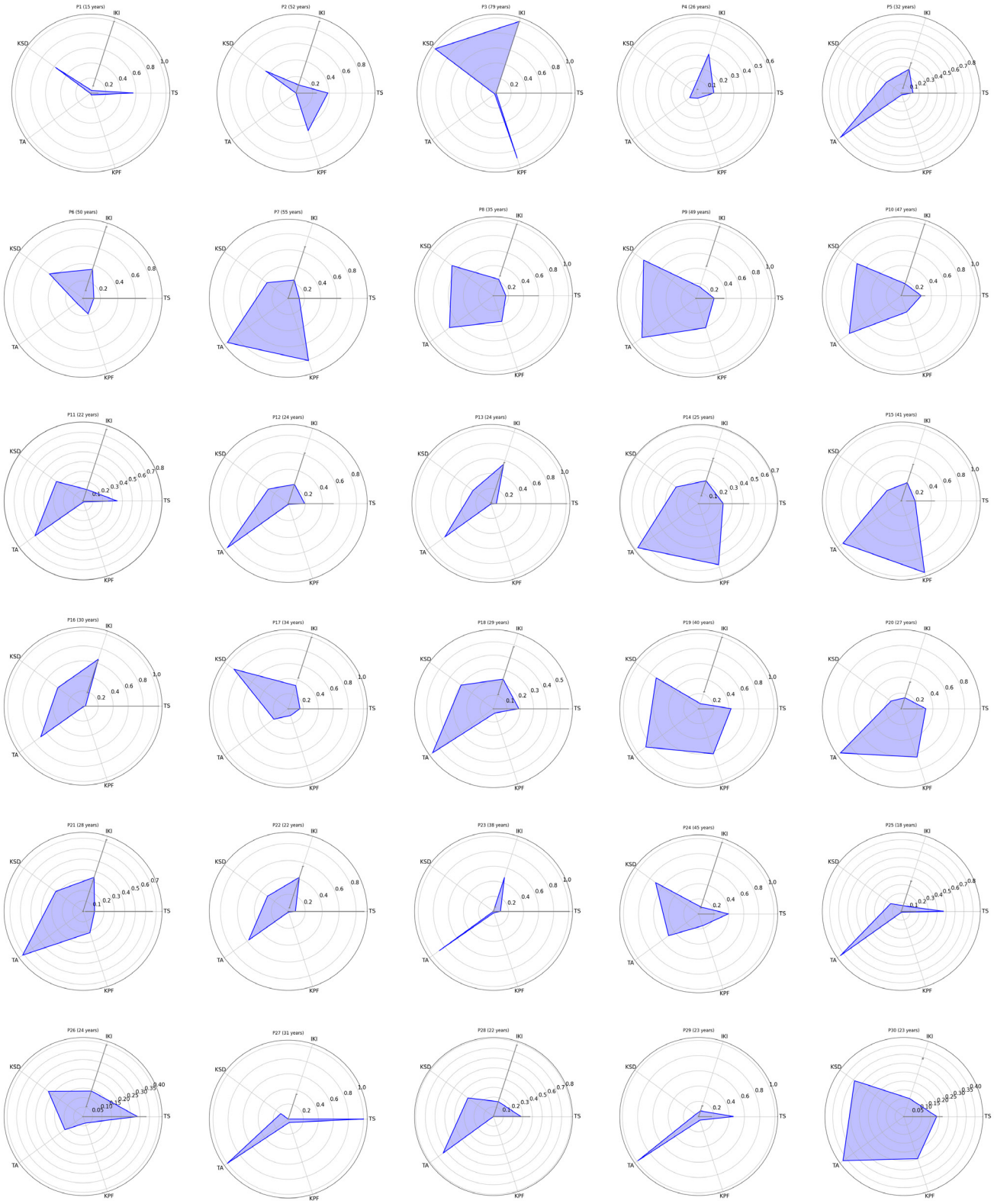


Figure 4. Unique typing signatures for all 30 participants (P1 to P30). Typing signatures generated by incorporating the normalized values of all five typing parameters for all 30 participants.

unique profile for every individual.

The significant correlations between age and keystroke dynamics—where older participants exhibited increased inter-key intervals, keystroke duration, and keypress force—can be explained by decreased motor control and slower reaction times associated with aging. Gender-based analysis revealed no statistically significant differences between males and females for any typing parameter, indicating that variations in typing measurements are not substantially affected by gender-related characteristics. Minor observed differences, such as males exhibiting slightly faster typing speeds and females demonstrating higher accuracy, may reflect anatomical differences and typing styles documented in ergonomic studies. Importantly, typing signatures maintained their discriminative power across these demographic groups, supporting the system's reliability for diverse user populations.

Several limitations must be considered when interpreting our findings. The controlled experimental environment in which data was collected may not fully represent real-world typing conditions. The repetitive typing of identical text by participants could potentially introduce biases related to memorization effects and limited typing pattern diversity. While statistical significance was achieved with the current sample size, broader generalizability could be enhanced through increased participant diversity across different typing proficiency levels and keyboard configurations. Additionally, while piezoelectric sensors performed well in recording typing metrics, other sensor technologies might provide better sensitivity and capture different types of data, such as distance travelled by each key when pressed, that could enhance typing signature profiles. It is also important to note that typing signatures, while promising, are not a complete solution; combining keystroke dynamics with other biometric methods such as voice or facial recognition could further

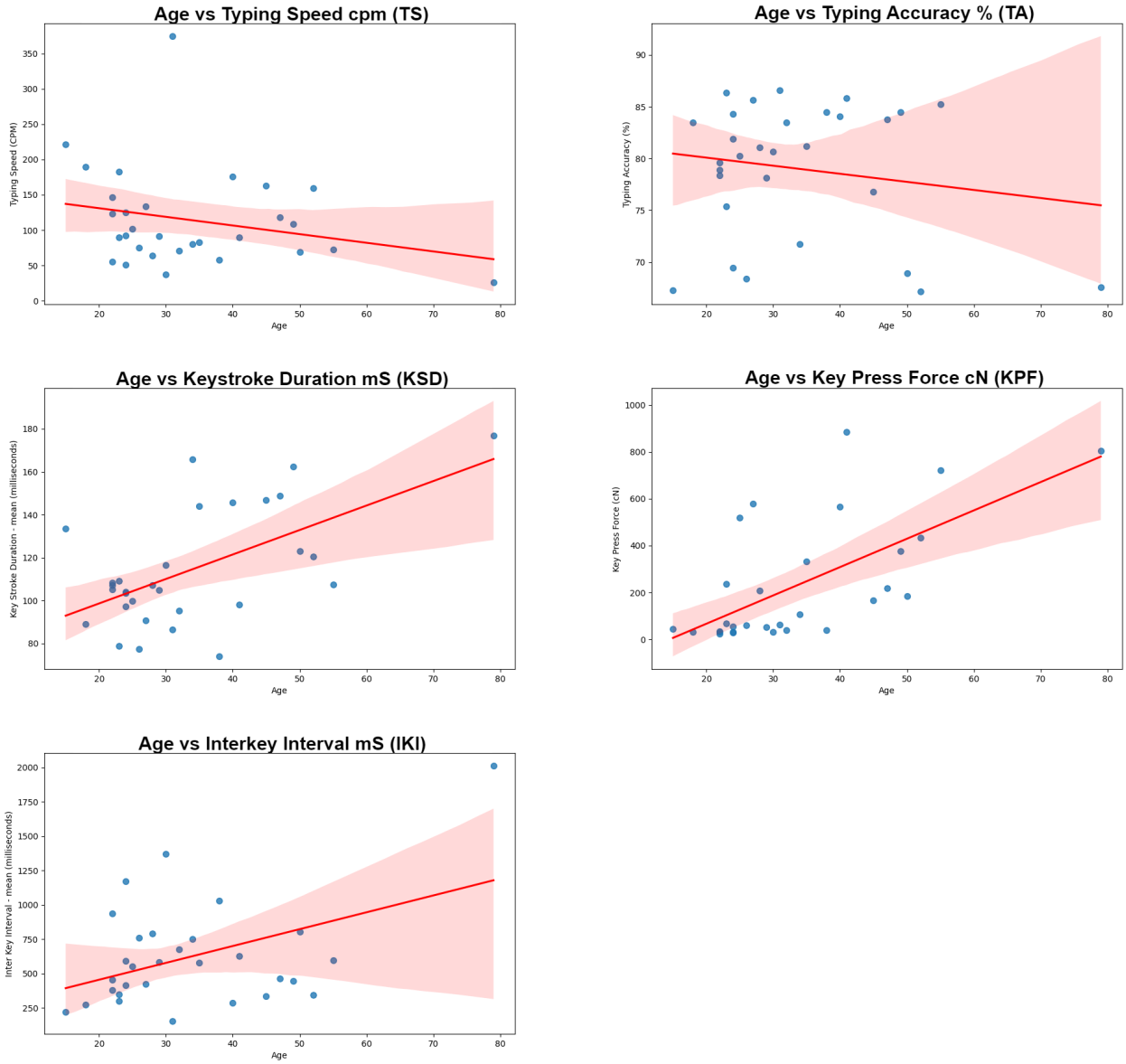


Figure 5. Variation of various keystroke parameters based on age. The correlation between age and different typing parameters is shown with linear regression lines (red) and 95% confidence intervals (red shaded regions).

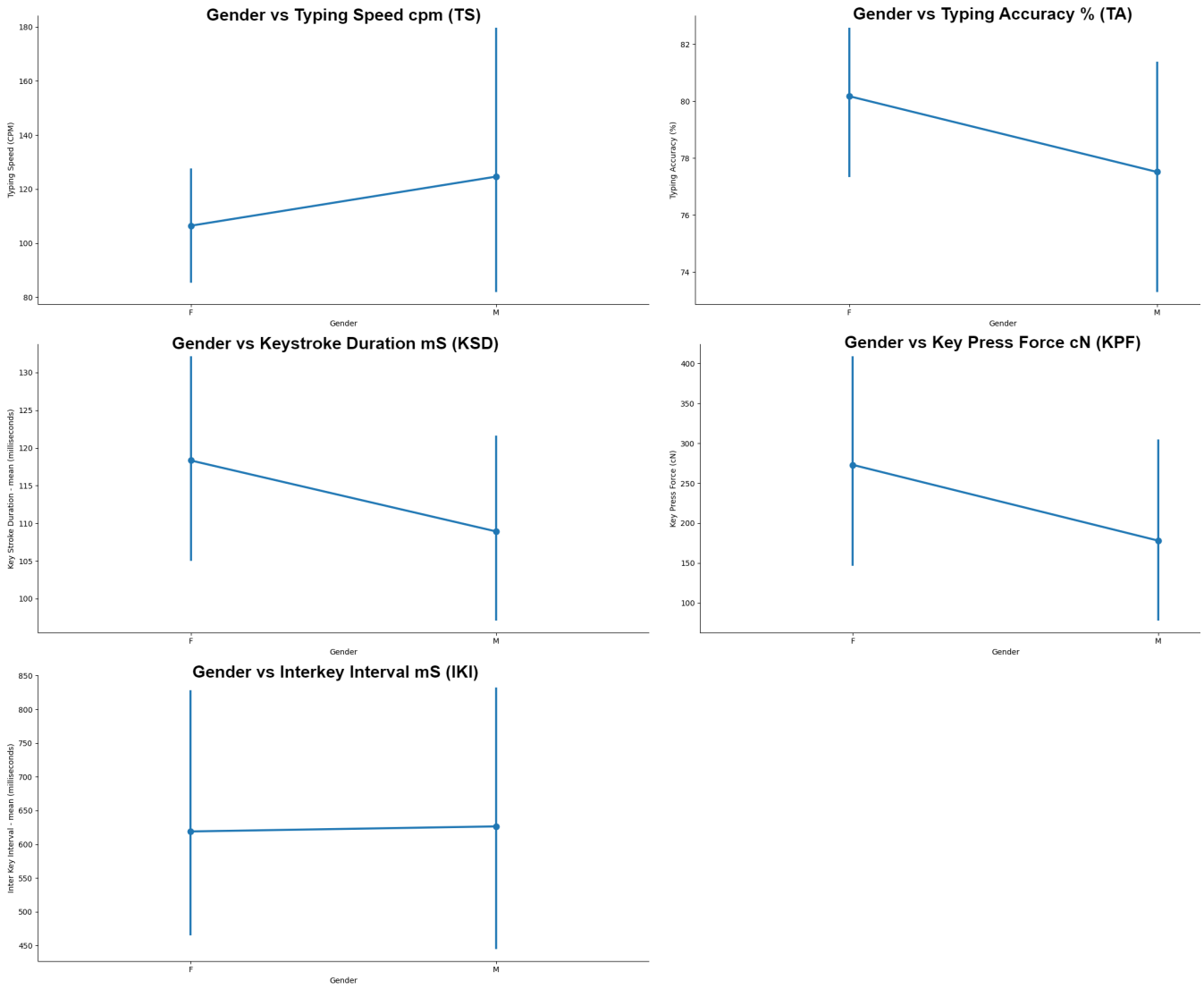


Figure 6. Variation of various keystroke parameters based on gender. The mean and the gender-associated variation of the different typing parameters based on gender.

improve system security.

Our findings highlight how typing signatures can transform digital security by offering a non-intrusive authentication method using specialized, cost-effective hardware. Several scientific questions remain for future investigation: How do changes in individual users, such as fatigue, affect typing patterns over extended periods? Can machine learning algorithms enhance the adaptability of typing signatures by learning and predicting changes in real time? Future research should focus on long-term studies assessing how typing signatures hold up over months or years, extending beyond fixed-text input to include naturalistic typing scenarios such as email composition and free-form writing, and evaluating system performance using only temporal metrics available from standard keyboards. These extensions would provide insights into the practical scalability of typing signature authentication. The practical applications of this technology extend to finance and healthcare, where data confidentiality is of utmost significance, offering a secure and accessible authentication solution for diverse user populations.

MATERIALS AND METHODS

Hardware setup

We developed a specialized keyboard with piezoelectric sensors that convert the amount of pressure applied into electrical signals. We strategically placed the sensors underneath each key of a traditional membrane-based keyboard. The sensors record the force applied by the user while pressing the keys and send this data to the connected computer in centinewtons. We attached each sensor to a grid form, which we then connected to an Arduino Uno microcontroller that helped to facilitate fast and cost-effective data collection.

Key typing parameters of keystroke dynamics

We considered several typing metrics, such as typing speed, inter-key intervals, keypress force, typing accuracy, and keystroke duration, in this study. These quantitative parameters are fundamental in building a biometric profile for every user in the form of a typing signature. The following sections contain the operational definitions of the various

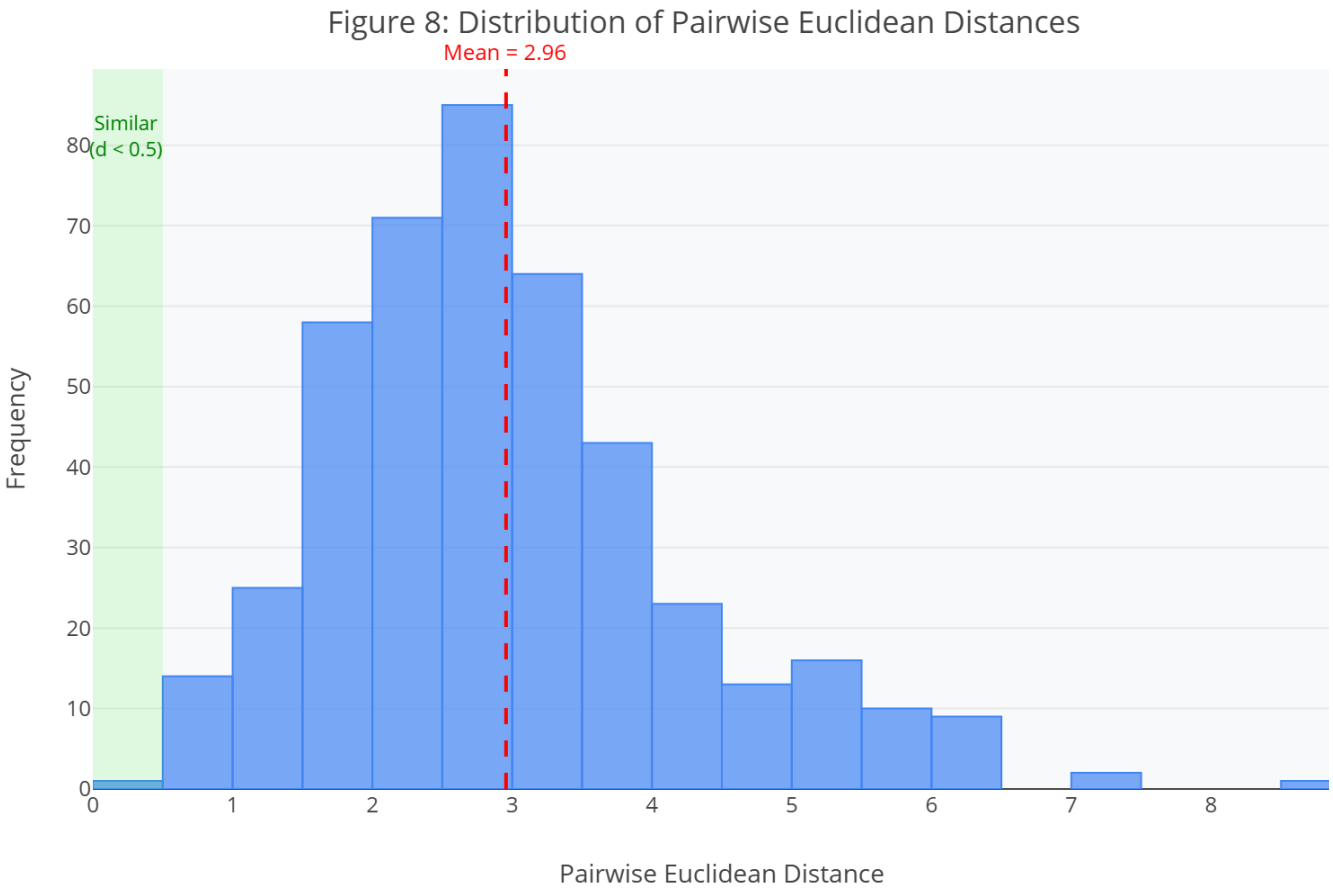


Figure 7. Distribution of pairwise Euclidean distances. Distribution of pairwise Euclidean distances between normalized typing signatures of all participants. The histogram shows 435 pairwise comparisons with a mean distance of 2.96 (red dashed line).

parameters:

Typing speed (TS) (characters per minute, CPM): Typing speed was defined as the rate at which an individual can enter text using a keyboard. It was quantified as the number of characters (including spaces and punctuation) typed per minute. This metric provides insights into a user's proficiency and efficiency in using a keyboard.

Inter-Key Interval (IKI) (milliseconds, ms): The inter-key interval was defined as the time duration between the release of one key and the pressing of the next key while typing. This measure helps to capture the rhythm and fluidity of a user's typing pattern, allowing for the identification of unique typing behaviours.

Keypress Force (KPF) (nentiNewtons, cN): Keypress force is defined as the amount of force applied by a user when pressing a key. This parameter provides insights into the user's typing style and pressure sensitivity, offering a behavioural biometric that can vary significantly from one person to another.

Typing Accuracy (TA) (%): Typing accuracy was defined as the proportion of correctly typed characters or words compared to a predetermined reference text. It reflects the precision of a user's typing ability, highlighting the frequency and nature of typing errors made during text entry.

Keystroke Duration (KSD) (milliseconds, ms): Keystroke duration was defined as the time duration for which a key remains pressed from the moment it is pressed down until it is released. This parameter can vary based on user habits and typing style, contributing to the uniqueness of a user's typing signature.

Data collection methodology

As the user typed, we used the hardware to record the keypress force data (cN) with the time at which the key was pressed for each keystroke and converted it into digital data, which we then stored in a CSV file. We developed a software application in Python 3.12 (35) to record other keystroke metrics. The resulting dataset was processed and analyzed using NumPy 1.26 (36), SciPy 1.12 (37), and visualized using Matplotlib 3.8 (38), with statistical measures displayed through various graphical representations, including bar charts, histograms, and heatmaps, to reveal patterns in typing behaviour (**Figure 3**).

Experiment design

We conducted a pilot study with 30 participants (P1 to P30) from various demographic natural traits and professional backgrounds. The sample size of 30 was selected based on established guidelines for pilot studies in biometric research, providing sufficient statistical power for preliminary analysis while remaining manageable for detailed data collection (32). The participant group consisted of persons aged 15 to 79, including 17 females and 13 males. We intentionally chose this diversity in participants to include a broad spectrum of

ID	Age	Sex	TS (CPM)	IKI - Mean (mS)	IKI - S.D. (mS)	KSD - Mean (mS)	KSD - S.D. (mS)	TA (%)	KPF - Mean (cN)
P1	22	F	55.14	936.20	100.240	105.13	23.31	78.38	30.36
P2	30	M	36.96	1367.80	131.190	116.64	21.67	80.68	30.45
P3	79	F	25.60	2011.20	205.480	176.74	58.05	67.57	805.19
P4	38	F	58.02	1031.00	119.020	74.05	14.12	84.46	39.60
P5	24	F	125.25	416.70	44.950	97.24	19.20	69.46	53.62
P6	24	M	51.30	1170.10	126.590	104.17	24.27	81.89	27.76
P7	49	F	108.72	447.60	48.350	162.47	30.63	84.46	377.35
P8	55	M	72.91	595.30	87.560	107.47	27.30	85.27	721.04
P9	32	M	71.08	674.10	73.340	95.17	18.17	83.51	38.77
P10	29	F	91.67	584.60	72.230	104.79	20.03	78.11	51.90
P11	18	F	189.20	274.70	25.300	89.06	20.96	83.51	31.23
P12	34	M	80.01	751.40	84.810	165.76	32.86	71.76	105.31
P13	22	M	123.68	452.50	48.660	107.32	32.22	79.59	22.35
P14	28	F	64.26	789.70	70.430	107.25	29.81	81.08	207.12
P15	35	F	82.89	578.90	79.420	143.98	30.14	81.22	331.28
P16	27	F	133.43	424.90	30.360	90.65	20.23	85.68	577.67
P17	41	F	89.58	627.30	43.430	98.06	24.23	85.81	884.66
P18	23	M	182.85	297.90	24.310	78.95	15.89	86.35	66.47
P19	52	M	159.64	345.70	34.960	120.39	32.55	67.16	433.03
P20	31	M	374.56	153.70	8.070	86.64	21.83	86.62	62.44
P21	45	F	163.10	333.00	29.400	146.77	40.41	76.76	166.15
P22	15	M	221.38	221.90	18.160	133.41	33.55	67.30	44.42
P23	26	M	74.68	758.90	62.140	77.31	11.20	68.38	59.96
P24	22	F	146.26	379.80	31.700	108.38	31.40	78.92	32.81
P25	47	F	118.04	463.60	35.270	148.73	45.16	83.78	218.64
P26	50	M	68.94	805.20	79.870	123.14	29.31	68.92	184.30
P27	40	F	175.83	285.10	31.610	145.68	32.79	84.05	565.69
P28	24	F	92.42	590.40	64.300	103.55	26.92	84.32	30.21
P29	25	M	101.91	550.90	53.570	99.72	19.46	80.27	519.32
P30	23	F	108.32	200.99	12.536	128.76	56.90	71.56	100.86

TS – Typing Speed, IKI – Interkey Interval, KSD – Keystroke Duration, TA – Typing Accuracy, KPF – Keypress Force

Table 1. Data collected from all the participants. The data recorded and processed for all five typing parameters for 30 different individuals using which the typing signature was generated.

backgrounds, comprising school pupils, college students, IT workers, homemakers, grandparents, and people with differing literacy skills. We made this selection to ensure the generalizability and robustness of our findings across various population segments. The non-equal gender distribution (17 females, 13 males) reflects the volunteer pool available for our study; while this may introduce some bias, our statistical analyses account for gender as a variable to assess any potential impact on the results.

Before starting the data collection, we provided each participant with a clear briefing about the study's goals, methods, and their roles as subjects in the study. We informed participants that their data would be kept confidential and that their contributions would only be used for research purposes. Participants signed a consent form before the start of the study. We designed the behavioural experiment while keeping the safety of participants in mind. We directed the participants to input a predetermined text given to them using the custom keyboard in the software interface provided to them. The text used was: "The quick brown fox jumps

over the lazy dog. Pack my box with five dozen liquor jugs. How vexingly quick daft zebras jump! Bright vixens jump; dozy fowl quack." This pangram-based text was structured to incorporate all the letters in the English language multiple times. We intentionally designed this to elicit the natural typing patterns of the user across the various keys in the keyboard. We chose a 10-minute typing session to ensure sufficient data collection while avoiding participant fatigue, based on ergonomic studies showing that typing performance remains stable within this timeframe (33).

We conducted the sessions in a controlled environment with minimal external distractions. The experimental setup consisted of Windows 10 operating system on desktop computers with our custom mechanical keyboards featuring integrated piezoelectric sensors. The environmental conditions, including lighting and sound, were maintained at constant levels, complemented by ergonomic seating configurations to enhance comfort and promote concentration throughout participation. We incorporated rest intervals into the study's protocol to mitigate the effects of muscular fatigue on typing performance. We conducted 6 separate sessions for each participant with intervals of 2–3 days between sessions to capture temporal consistency while avoiding learning effects. We attempted to achieve typing metrics by implementing alternating typing sessions and rest intervals.

Data analysis and processing

We transmitted the data via a serial link to a networked computer for processing. We employed Python 3.12 for data analysis due to its extensive array of libraries and adaptability in managing data processing tasks (**Table 1**) (35). We carried out statistical analysis on the data using NumPy 1.26 to calculate essential metrics such as mean and standard deviation, and SciPy 1.12 for t-tests and Pearson correlation analysis (36, 37). We visualized the resulting statistical measures, such as bar charts, histograms, and heat maps, using Matplotlib 3.8 (38). We then pictorially depicted the statistical measures of the five typing parameters as a polygon using a spider or radar plot along its axes. Each polygon represented the typing signature of an individual.

Statistical analyses

We have included the Coefficient of variation analysis for assessing within-participant consistency, pairwise Euclidean distance calculations using z-score normalized features for uniqueness assessment, independent sample t-tests for gender comparisons (two-tailed, $\alpha = 0.05$), Pearson correlation coefficients with significance testing for age relationships and further more critical t-value of ±2.048 ($df = 28$, $p = 0.05$) was used for all significance determinations.

ACKNOWLEDGMENTS

We would like to acknowledge the support of Ms. Aashna Saraf (CreatED) who provided the platform to support this research work.

Received: February 13, 2025
Accepted: March 22, 2026
Published: June 08, 2026

REFERENCES

1. Bours, Patrick. "Continuous Keystroke Dynamics: A Different Perspective Towards Biometric Evaluation." Information Security Technical Report, vol. 17, no. 1–2, Feb. 2012, pp. 36–43, https://doi.org/10.1016/j.istr.2012.02.001.
2. Crawford, Heather. "Keystroke dynamics: Characteristics and opportunities." International Conference on Privacy, Security and Trust, 8th ed., IEEE, 2010, pp. 205–12, https://doi.org/10.1109/pst.2010.5593258.
3. Bonneau, Joseph, et al. "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes." IEEE Symposium on Security and Privacy, IEEE, 2012, pp. 553–67, https://doi.org/10.1109/SP.2012.44.
4. Button, Mark, et al. "Online Frauds: Learning from Victims Why They Fall for These Scams." Australian & New Zealand Journal of Criminology, vol. 47, no. 3, 2014, pp. 391–408, https://doi.org/10.1177/0004865814521224.
5. Cross, Cassandra. "Victims' Responses to Online Fraud: An Examination of Psychological Impact and Detriment." Crime Prevention and Community Safety, vol. 20, no. 2, 2018, pp. 108–24, https://doi.org/10.1057/s41300-018-0041-z.
6. Dias, Tiago, et al. "KeyRecs: A Keystroke Dynamics and Typing Pattern Recognition Dataset." Data in Brief, vol. 50, Aug. 2023, p. 109509, https://doi.org/10.1016/j.dib.2023.109509.
7. González, Nahuel. "Dataset for Towards Liveness Detection in Keystroke Dynamics: Revealing Synthetic Forgeries." IEEE DataPort, vol. 1, 19 May 2021, https://doi.org/10.17632/xvg5j5z29p.1.
8. Karnan, M., et al. "Biometric Personal Authentication Using Keystroke Dynamics: A Review." Applied Soft Computing, vol. 11, no. 2, Aug. 2010, pp. 1565–73, https://doi.org/10.1016/j.asoc.2010.08.003.
9. Kasprowski, Pawel, et al. "Biometric Identification Based on Keystroke Dynamics." Sensors, vol. 22, no. 9, Apr. 2022, p. 3158, https://doi.org/10.3390/s22093158.
10. Biggio, Battista, and Fabio Roli. "Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning." Pattern Recognition, vol. 84, 2018, pp. 317–31, https://doi.org/10.1016/j.patcog.2018.07.023.
11. Peacock, A., et al. "Typing Patterns: A Key to User Identification." IEEE Security & Privacy, vol. 2, no. 5, Sept. 2004, pp. 40–47, https://doi.org/10.1109/msp.2004.89.
12. Pisani, Paulo Henrique, and Ana Carolina Lorena. "A Systematic Review on Keystroke Dynamics." Journal of the Brazilian Computer Society, vol. 19, no. 4, July 2013, pp. 573–87, https://doi.org/10.1007/s13173-013-0117-7.
13. Roth, Judith, et al. "Biometric Authentication via Keystroke Sound." International Conference on Biometrics, IEEE, 2013, pp. 1–8, https://doi.org/10.1109/ICB.2013.6613015.
14. Monrose, Fabian, and Aviel D. Rubin. "Keystroke Dynamics as a Biometric for Authentication." Future Generation Computer Systems, vol. 16, no. 4, 2000, pp. 351–59, https://doi.org/10.1016/S0167-739X(99)00059-X.
15. Banerjee, Salil P., and Damon L. Woodard. "Biometric Authentication and Identification Using Keystroke Dynamics: A Survey." Journal of Pattern Recognition Research, vol. 7, no. 1, 2012, pp. 116–39, https://doi.

org/10.13176/11.427.
16. Alsultan, Arwa, and Kevin Warwick. "Keystroke Dynamics Authentication: A Survey of Free-text Methods." International Journal of Computer Science Issues, vol. 10, no. 4, 2013, pp. 1–10.
17. Chang, Tzu-Yu, et al. "A Novel Security Scheme for Behavioral Authentication Systems Based on Keystroke Dynamics." Security and Communication Networks, vol. 2019, 2019, https://doi.org/10.1002/spy2.64.
18. Trojahn, Matthias, and Frank Ortmeier. "Toward Mobile Authentication with Keystroke Dynamics on Mobile Phones and Tablets." International Conference on Advanced Information Networking and Applications Workshops, IEEE, 2013, pp. 697–702, https://doi.org/10.1109/WAINA.2013.36.
19. Idrus, Syed Zulkarnain Syed, et al. "Soft Biometrics for Keystroke Dynamics: Profiling Individuals While Typing Passwords." Computers & Security, vol. 45, June 2014, pp. 147–55, https://doi.org/10.1016/j.cose.2014.05.008.
20. Loy, Chen Change, et al. "Keystroke Patterns Classification Using the ARTMAP-FD Neural Network." International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2007), 3rd ed., IEEE, 2007, pp. 61–64, https://doi.org/10.1109/iih-msp.2007.218.
21. Maalej, Aicha, et al. "Investigating Keystroke Dynamics and Their Relevance for Real-Time Emotion Recognition." SSRN Electronic Journal, Jan. 2022, https://doi.org/10.2139/ssrn.4250964.
22. Ali, Muhammad Lutfi, et al. "Keystroke Biometric Systems for User Authentication Using Deep Learning Techniques." IEEE Access, vol. 9, 2021, pp. 41354–72, https://doi.org/10.1109/ACCESS.2021.3064762.
23. Ayotte, Blaine, et al. "Fast Free-Text Authentication via Instance-Based Keystroke Dynamics." IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 2, no. 4, 2020, pp. 377–87, https://doi.org/10.1109/TBIOM.2020.3005616.
24. Monaco, John V. "Robust Keystroke Biometric Anomaly Detection." arXiv preprint arXiv:1606.09075, 2016, https://doi.org/10.48550/arXiv.1606.09075.
25. Raul, Nataasha, et al. "A Comprehensive Review of Keystroke Dynamics-Based Authentication Mechanism." Advances in Intelligent Systems and Computing, Nov. 2019, pp. 149–62, https://doi.org/10.1007/978-981-15-0324-5_13.
26. Serwadda, Abdul, and Vir V. Phoha. "Examining a Large Keystroke Biometrics Dataset for Statistical-Attack Openings." ACM Transactions on Information and System Security, vol. 16, no. 2, Sept. 2013, pp. 1–30, https://doi.org/10.1145/2516960.
27. Sun, Yan, et al. "Shared keystroke dataset for continuous authentication." IEEE International Workshop on Information Forensics and Security (WIFS), IEEE, 1 Dec. 2016, pp. 1–6, https://doi.org/10.1109/wifs.2016.7823894.
28. Teh, Pin Shen, et al. "A Survey of Keystroke Dynamics Biometrics." The Scientific World JOURNAL, vol. 2013, no. 1, Jan. 2013, https://doi.org/10.1155/2013/408280.
29. Tey, Chee Meng, et al. "I Can Be You: Questioning the Use of Keystroke Dynamics as Biometrics." Network and Distributed System Security Symposium, Jan. 2013, p. 1, flyer.sis.smu.edu.sg/ndss13-tey.pdf.
30. Schmidt, Richard A., and Timothy D. Lee. Motor Control and Learning: A Behavioral Emphasis. Human Kinetics, 5th ed., 2011.
31. Trewin, Shari. "Physical Usability and the Mobile Web." International Cross-Disciplinary Conference on Web Accessibility, ACM, 2006, pp. 109–12, https://doi.org/10.1145/1133219.1133239.
32. Julious, Steven A. "Sample Size of 12 per Group Rule of Thumb for a Pilot Study." Pharmaceutical Statistics, vol. 4, no. 4, 2005, pp. 287–91, https://doi.org/10.1002/pst.185.
33. Galinsky, Traci L., et al. "A Field Study of Supplementary Rest Breaks for Data-Entry Operators." Ergonomics, vol. 43, no. 5, 2000, pp. 622–38, https://doi.org/10.1080/001401300184297.
34. Zhong, Yu, and Yunbin Deng. "A Survey on Keystroke Dynamics Biometrics: Approaches, Advances, and Evaluations." Gate to Computer Science and Research, 2015, pp. 1–22, https://doi.org/10.15579/gcsr.vol2.ch1.
35. Van Rossum, Guido, and Fred L. Drake. Python 3 Reference Manual. CreateSpace, 2009.
36. Harris, Charles R., et al. "Array Programming with NumPy." Nature, vol. 585, no. 7825, Sept. 2020, pp. 357–62, https://doi.org/10.1038/s41586-020-2649-2.
37. Virtanen, Pauli, et al. "SciPy 1.0: Fundamental Algorithms for Scientific Computing in Python." Nature Methods, vol. 17, no. 3, 2020, pp. 261–72, https://doi.org/10.1038/s41592-019-0686-2.
38. Hunter, John D. "Matplotlib: A 2D Graphics Environment." Computing in Science & Engineering, vol. 9, no. 3, 2007, pp. 90–95, https://doi.org/10.1109/MCSE.2007.55.