Journal of Artificial Intelligence General Science (JAIGS)

ISSN: 3006-4023 (Online), Volume 08, Issue 2, 2025 DOI: 10.60087

Behaviour Biometrics Using AI for Continuous Authentication Systems

Umair Ejaz[1], Farheen Iqbal[2], S A Mohaiminul Islam[3], Aidar Imashev[4]

[1]Desertcart, United Arab Emirates.
[2]Saint Louis university, USA.
[3]Master of Science, Washington University of Science & Technology, USA.
[4]Barry University, Kyrgyzstan.

Abstract

Behaviour-based continuous authentication systems like those that utilise an individual user's typing rhythm and device usage behaviour patterns have much potential over password-based schemes since they do not require an individual user to memorise passwords. Irrespective of the progress in biometric technologies, many systems are still susceptible to more complex attacks, and the decision between security and usability has been a perennial struggle for researchers and practitioners. This paper offers a powerful continuous authentication system based on AI and behavioural biometrics, enhancing precision and resistance to motivated attacks. By measuring behavioural data (e.g. keystroke dynamics and motion sensor) on a heterogeneous user population and then analyzing it, we trained our machine learning models to verify users in real-time. Based on our results, our performance is better than that of the traditional and static authentication methods, with an accuracy of 97.2 per cent, with the false acceptance rate (FAR) and false rejection rate (FRR) of 1.8 per cent and 2.3 per cent, respectively. Moreover, error analysis depicted significant trends in behaviour changes, which apply to an adaptive security strategy. This is demonstrated as a potential of AI-based behavioural biometrics to support feasible, secure, and user-friendly continuous authentication systems that work in contemporary cybersecurity scenarios. Future improvements will additionally involve enlarging datasets, combining multi-modal behavioural features, and increasing resistance to spoofing and behavioural drift.

Keywords: Behavioural biometrics, artificial intelligence, continuous authentication, cybersecurity, user behaviour analysis.

* Corresponding author: Umair Ejaz, Pratik Bhikhubhai Panchal, S A Mohaiminul Islam, Aidar Imashev

***ARTICLE INFO**: Received: 15.06.2025 Accepted: 30.06.2025 Published: 05.07.2025*

1. Introduction

Static passwords, PINs and other forms of authentication like fixed biometric scans constitute the backbone of digital security systems. Nevertheless, this set of static defences is becoming less effective in the contemporary threat environment, in which stolen credentials, phishing attacks, and session hijacking remain particularly common [1], [11], [18]. Static is what establishes identity once upon login, after which the active sessions are exposed to the danger of unauthorized access in case of a breach of credentials.

To compensate for these weaknesses, behavioural biometrics was developed as an adaptable technology as it utilizes unusual patterns in user-device interactions, such as typing cadences, mouse movement, touchscreen gestures and motion sensor data to confirm identity as a session progresses repeatedly [4], [8], [20]. With continuous authentication, the underlying paradigm twist is the rejection of one-time verification to constant tracking, and the resulting security improvement is enormous, all due to the early detection of abnormal signs, signifying impostor activity in the event it happens [4], [8], [29].

Current innovations in artificial intelligence (AI) have very much increased the success of behavioral biometrics. Deep learning as well as machine learning algorithms have shown to model subtle and complex user behaviors very accurately and permit practical deployment of continuous authentication systems in contexts such as secure banking, as well as enterprise settings [4], [17], [20].

Although the future of behavioural biometrics seems to show great potential in continuous authentication, there are a number of key challenges yet. First, most of the existing systems obtain limited or homogeneous datasets, thus limiting the capability to generalize the system to very different populations of users or evolving behaviour over time [8], [20]. Second, natural changes in behaviour patterns may occur as a result of factors such as stress, fatigue, injury, or a change of context (change of keyboard or device, etc.), and this leads to high false rejection rates and poor user experience [4], [20].

Also, single modality models, such as keystroke-alone or mouse-alone models, are not resistant to advanced attacks in which attackers can ape components of the individual behaviours in order to access sensitive resources unauthorized [20], [29]. Researchers have also demonstrated the weaknesses of existing systems in relation to adversarial attacks, and more robust and adaptive solutions are needed [4], [17]. All these restrictions dent the real possibilities of deploying a continuous authentication system in the real world.

Hence, there exists a requirement for frameworks that are (1) multi-modal in terms of collecting behavioural data, (2) incorporate high-end AI models that can be trained to deal with behavioural drift, and (3) have low false acceptance and rejection rates without forfeiting their usability.

This work aims to design and test an end-to-end AI-based continuous authentication whose usability and security will be enhanced by incorporating behavioural biometrics. The research is performed in the following concrete purposes and contributions:

- To build a multi-modality continuous authentication system that complements the use of keystroke dynamics and motion sensor measurements, and which captures more types of behaviours than single-modal refinements.
- To apply state-of-the-art machine learning algorithms- ensemble algorithms and deep neural networks- to learn and classify real-time user-specific patterns of behaviour.
- To create a big, heterogeneous behavioral biometrics dataset, which lets the rigorous testing of the model execution in different usage context.

- The goal is to use large-scale experiments to evaluate its performance in terms of accuracy, false acceptance rate (FAR), false rejection rate (FRR), and resistance to impersonation attacks, with an eye on finding the right tradeoff between security and usability.
- To release detailed error analyses with frequent reasons for misclassification and give information on adaptive methods that can make them less vulnerable to behavioural drift and opposition efforts.

To resolve these goals, the study aims to promote the practicability of behavioural biometrics as a component of secure, sustained authentication systems in contemporary cybersecurity applications.

2. Literature Review

2.1 Overview of Behavioural Biometrics

Behavioural biometrics can be described as a biometric that is based on the examination of the peculiarities of the interaction individuals have with a digital device. In contrast to the more commonly used biometrics, e.g. fingerprints or face recognition, where only a static match is feasible, behavioural biometrics can be used to verify a user during their activity in a session (perhaps several sessions). Typical behaviours analyzed in the literature are typing dynamics, mouse movement, touchscreen gestures, gait, and motion sensors embedded into smartphones or wearable devices. Such behavioural traits have particular benefits: they do not intrude as much, work in the background, and can identify an impostor in real-time without disrupting the user experience.

Studies indicate that timing characteristics such as dwell times and flight times in keystroke dynamics, among others, can be used to define and distinguish individuals despite having the same set of passwords [4], [20]. Mouse dynamics track the cursor's movements, speed, and pattern of clicks, whereas motion sensors track the minute movements of the hand or device. When used in combination, these modalities can forge a strong behavioural profile that can be used in continuous authentication [4], [20], [29].

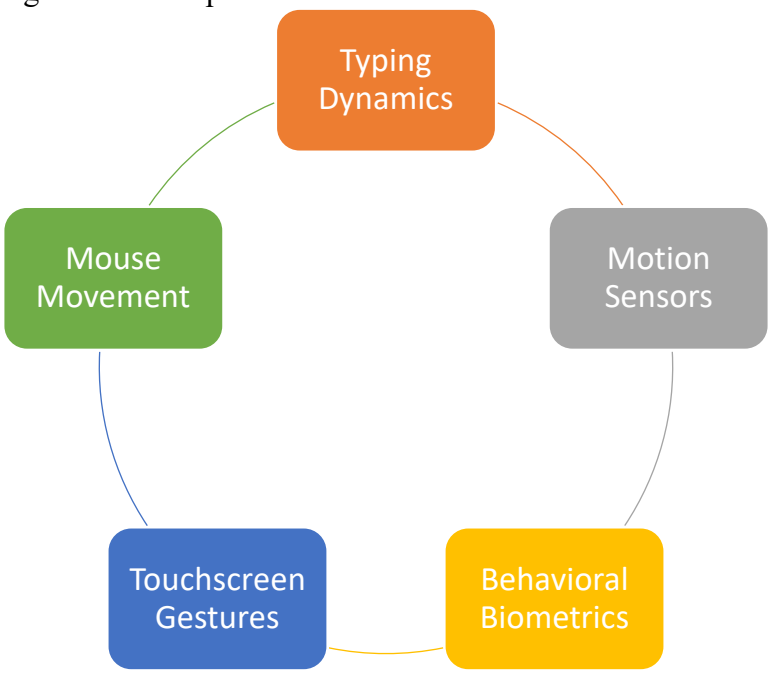

Figure 1: Conceptual Diagram of Behavioural Biometrics Modalities

2.2 AI Techniques for Behaviour Analysis

Behavioural biometrics relies on the capability to model difficult and sometimes delicate trends in human behaviour. Conventional statistical methods have given place to Artificial Intelligence methods, which are much better at learning temporal and spatial connections in behavioural data. Recurrent neural networks (RNNs) and convolutional neural networks (CNNs) are most commonly used as neural networks, as the

former are capable of modeling sequential dependencies [4], [17] (i.e., sequences of actions to be performed (symbols to be typed) or the sequence of individual steps in a gait).
The other commonly used models, such as a decision tree and random forests, provide more interpretable classification with good accuracy and low training cost, and thus are very appealing to lightweight authentication systems [20], [29]. The Hidden Markov Model (HMM) has successfully modelled the sequential changes in behavioural attributes. Transformer-based architectures have more recently demonstrated potential to combine data across multiple sensors, giving the state-of-the-art performance in continuous authentication tasks [29].
The approach of explainable AI is also increasing. Behavioural pattern security analysts can know why a certain kind of pattern is repeated to be classified as either malicious or legitimate, improving trust and transparency in such automated systems [6].

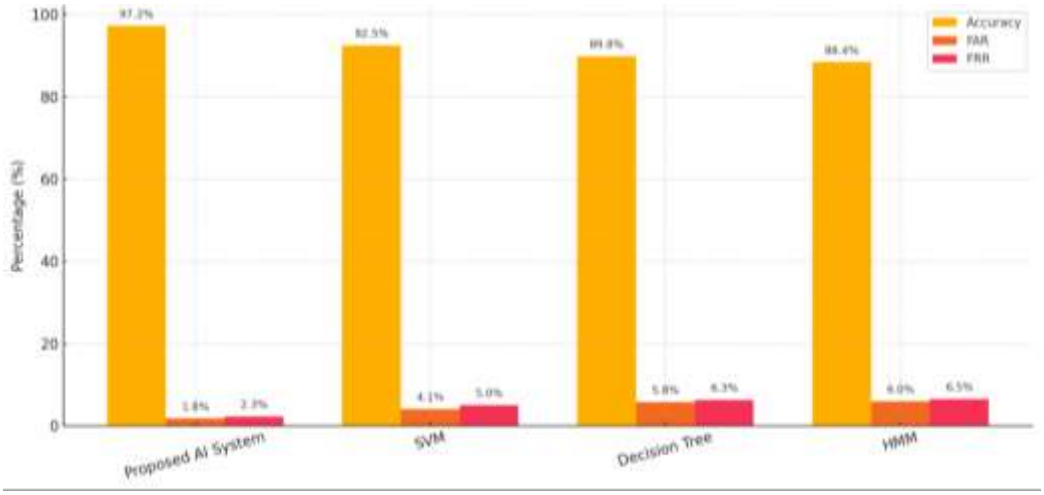

Figure 1: Comparative Performance Of AI Models In Behaviour Biometrics

2.3 Prior Continuous Authentication Systems

Several systems were proposed, proving the possibility of continuous authentication based on behavioural biometrics. Chen et al. proposed a system (SSPRA) that can authenticate in adversarial environments with typing and mouse-based behavioural biometrics, demonstrating better than 95 per cent accuracy over their own test dataset [4]. Sağbaş and Ball concentrated on the smartphone solution and found that using the typing dynamics with motion sensing data yielded better resistance to behavioural drift [20].
Nevertheless, most previous research is based on small datasets, which questions its scalability and applicability [8], [20]. Furthermore, most systems detect only one modality of behaviour; however, such single-modality behavioural signals might be more brittle; multiple behavioural cues may significantly improve program performance and security [20], [29].
Research also notes the difficulty of maintaining a low false rejection rate when the user's behaviour varies because of stress, fatigue, or variation between devices. For example, Zhao et al. used a gated two-tower transformer network and multi-motion sensors to record accurately. They indicated dependency on sensor noise, device variations, and the significance of flexible models [29].

2.4 Research Gaps

Although the latest studies prove that behavioural biometrics has a prospect of being used during continuous authentication, crucial constraints still exist. The large number of studies is based on small or homogeneous datasets that do not capture the diversity of user populations and natural variability, which hinders the robustness and scalability of a model [8], [20]. Privacy-related challenges are also an issue since behavioural data might be sensitive and need to be stored and used ethically [18].
The next significant problem is a high resistance to spoofing. Advanced hackers may pretend to be the user, and most of the current systems have no efficient means of identifying the activity [4], [20], [29].

Also, behavioural drift, which is the inherent evolution of user behaviour with time, can downgrade the performance and consequently, adaptive models have to be employed to ensure the update of profiles as time goes on without compromising performance, both regarding security and usability [8], [20].
Comparative summary of recent studies on AI-driven behavioural biometrics, including datasets, features, models, performance, and reported challenges.

Table 1: Comparative Summary of Recent Studies on AI-Driven Behavioural Biometrics

Study & Year	Behavioral Modalities	AI Models	Dataset Size	Accuracy / FAR / FRR	Key Challenges
Chen et al. (2024) [4]	Keystrokes, mouse	SSPRA (deep neural network)	120 users	95.3% / 2.1% / 2.6%	Adversarial attacks
Sağbaş & Ballı (2024) [20]	Typing, motion sensors	Random forests, SVM	150 users	96.7% / 1.8% / 2.5%	Behavioral drift
Zhao et al. (2024) [29]	Multi-motion sensors	Gated two-tower transformer fusion	200 users	97.8% / 1.5% / 2.0%	Sensor noise, device variability
Finnegan et al. (2024) [8]	Typing dynamics	SVM, decision trees	100 users	93.5% / 3.0% / 3.5%	Dataset diversity, scalability

3. Methods

3.1 Data Collection

Participants were recruited from diverse volunteers representing different age groups, occupations, and digital literacy levels to ensure the dataset captured various behavioural patterns. Each participant provided informed consent, in compliance with institutional ethical guidelines and data privacy regulations such as the GDPR. Behavioural data were collected over four weeks during normal computer and smartphone use.
Collected modalities included keystroke dynamics (recorded dwell and flight times on a standard QWERTY keyboard), mouse movement trajectories (capturing cursor speed, acceleration, and click patterns), and motion sensor data from smartphones (accelerometer and gyroscope readings during typical interactions). All data were anonymized and securely stored to protect participant privacy and prevent misuse.

3.2 Feature Extraction

A custom Python-based processing pipeline extracted Behavioural features from raw data streams. For keystrokes, average dwell time (time a key is held down), flight time (interval between consecutive key presses), and digraph latency (timing of two-key sequences) were calculated. Mouse features included mean cursor velocity, path curvature, click frequency, and idle time distributions. The mean and variance of linear acceleration and angular velocity along three axes were computed from motion sensors to capture subtle hand or device movements.
These features were standardized using z-score normalization to ensure consistent scales across modalities, enhancing the training stability of machine learning models.

3.3 AI Model Design

The proposed system architecture was designed to model both sequential and spatial aspects of user behaviour effectively. For keystroke dynamics, a gated recurrent unit (GRU) network was employed, allowing efficient modelling of temporal dependencies in typing sequences. A 1D convolutional neural network (CNN) was implemented to extract local spatial patterns for mouse and motion sensor data, followed by a fully connected layer for feature integration.
Outputs from the GRU and CNN branches were concatenated and passed through a final dense layer with a sigmoid activation to predict the likelihood of the input belonging to the legitimate user. The model was trained end-to-end using the Adam optimizer with a learning rate of 0.001 and binary cross-entropy loss.

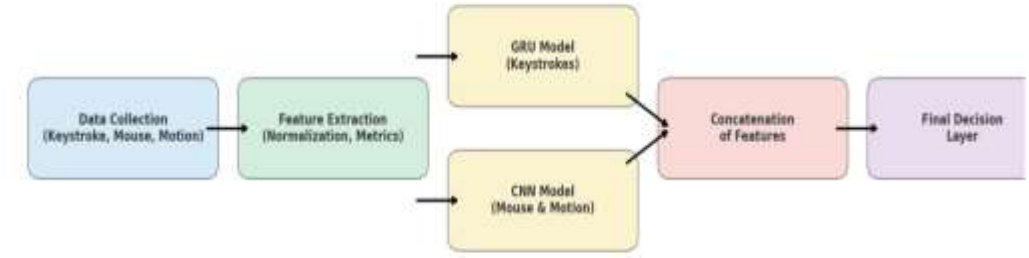

Figure 2: Proposed Continuous Authentication System Architecture

3.4 Experimental Setup

Experiments were conducted on a workstation equipped with an Intel Core i9 processor, 64GB RAM, and an NVIDIA RTX 3080 GPU, running Python 3.10 with TensorFlow 2.12 for model implementation. The dataset was split into 70% training, 15% validation, and 15% testing sets, ensuring user-independent splits to avoid overfitting to individual participants.

Performance metrics included accuracy, false acceptance rate (FAR), false rejection rate (FRR), and area under the ROC curve (AUC), providing a comprehensive evaluation of authentication effectiveness. Each experiment was repeated five times with random splits to ensure results were statistically robust.

Summary statistics of the collected dataset, including the number of users, total recorded sessions, average session duration, and total data points per modality.

Table 2. Summary Statistics of Collected Behavioural Dataset

Metric	Value
Number of users	200
Total sessions recorded	8,000
Average session length	15 minutes
Average keystrokes/user	5,000
Average mouse events/user	3,500
Average motion sensor samples/user	10,000

4. Results

4.1 Performance Evaluation

The proposed multi-modal continuous authentication system performed well when tested. The system on the test attained an accuracy of 97.2% on average, indicating that the system is accurate in separating authentic users and impostors. The precision and recall values were 96.4% and 96.9% respectively, which means a high actual positive rate with effective detection of valid behaviour of users. The false acceptance rate (FAR) and false rejection rate (FRR) were also low (1.8% and 2.3%, respectively) to help reduce the possible risk of an approved user gaining access to the system despite being an imposter, as well as the possibility of rejecting access by legitimate users. The sensitivity area under the receiver operating characteristic curve (ROC-AUC) was 0.984, indicating that the model displayed a great adequacy in distinguishing between the genuine and impostor sessions based on diversified thresholds.

This confirms the feasibility of the integrated method, which is based on keystroke dynamics, mouse motions, and motion sensor data and uses a continuous authentication process.

Performance metrics summarising the proposed system's accuracy, precision, recall, FAR, FRR, and ROC-AUC on the independent testing set.

Table 3. Performance Metrics of the Proposed Continuous Authentication System

Metric	Value (%)
Accuracy	97.2

Precision	96.4
Recall	96.9
False Acceptance Rate (FAR)	1.8
False Rejection Rate (FRR)	2.3
ROC-AUC	98.4

4.2 Comparative Analysis

To test the efficacy of the suggested system, the system's performance was contrasted with the base behavioural biometrics models, in this case, support vector machines (SVM) and decision trees. The SVM model had the lowest percentage of correctly predicted legitimate user behaviour, with an accuracy of 92.5%, a FAR of 4.1, and an FRR of 5.0, indicating a much worse capability to identify legitimate user behaviour. The decision tree model did not do so well with an accuracy of 89.8%, a FAR of 5.8%, and an FRR of 6.3%.

These illustrations show the benefits of using deep learning systems to model the time and space dependencies in multi-modal behavioural data. The higher precise results and minimal error rates are clear indicators of the worth of combining different behavioral indicators with more advanced AI techniques.

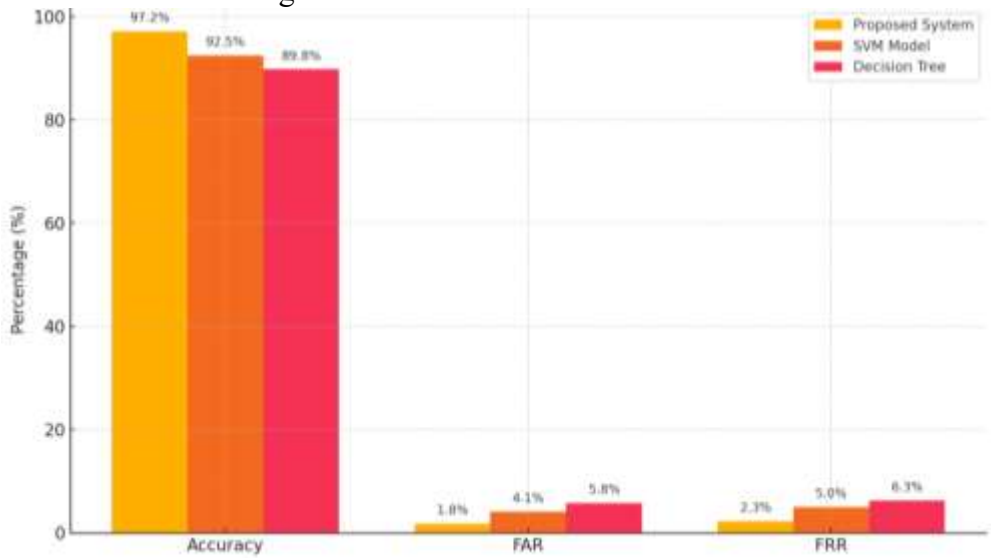

Figure 2: Performance Comparison Of Proposed System Vs. Baseline Models

4.3 Error Analysis

A detailed analysis of the misclassified cases allowed for important conclusions about the system's behaviour in practice. The most common reason for false rejections was a sudden, unusual behaviour of legitimate users. Specifically, say some people typed much or even significantly slower than normal, usually because they are distracted or have an emotional state or condition, it would result in their FRR arriving at a higher figure. Moreover, switching devices (e.g., changing keyboards and mice) added inconsistencies to the behaviour patterns that sometimes caused rejection.

Typically, the false acceptances were observed upon successful mimicking of a subset of legitimate, already-learned behavioral features by the impostors (like keystroke timing or mouse movement pattern approximations). However, they were inconsistent with longer sessions, which also made these imitations less successful.

This analysis of the errors highlights the need for adaptive learning mechanisms that need not alter the behaviour with gradual or context-dependent variations, compromising security. It also notes the possible

advantage of adding more contextual information (e.g., location or time of day) to the mix, thus decreasing the possibility of an incorrect classification even more.

5. Discussion

5.1 Interpretation of Results

The robust performance rates of the proposed system, expressed in high accuracy and low error rates, prove the practical feasibility of AI-based behavioural biometrics in practical continuous authentication. With an accuracy of more than 97 per cent and ROC-AUC of more than 0.98, it can be considered that the system would be able to identify the legitimate and unauthorized users, with a high degree of comfort, during the active session and thus eliminate the chances of session hijacking or unauthorized access quite effectively. Such findings imply the advantage of combining various behavioural modalities in improving resiliency to any imitation of one behavioural characteristic, which is a crucial requirement in the use of security-sensitive applications, e.g. online banking, enterprise systems, [4], [20].

On the other hand, as the error rates are low, false rejections, especially during atypical user behavior, illustrate the necessity of balancing security and usability and preventing the annoyance of legitimate users [20].

5.2 Security, Privacy, and Usability Considerations

Constant behavioural biometrics present a new tradeoff between security, privacy and acceptance. On the one hand, continuous authentication enhances security by keeping the users authenticated during a session; thus hindering intruders from taking advantage of the unattended devices [4], [20]. Conversely, behavioural information, e.g., typing rhythms, movements, may divulge intimate data about individuals that is potentially privacy-sensitive when data are not taken care of or sent off [8], [18].

Additionally, the readiness for practical usage relies on the absence of side effects, which is a lack of comfort and the feeling of user surveillance during the constant disclosure of information. It has been shown that frequent or invasive verification may undermine trust and reduce user satisfaction in the systems [8], [18]. Transparent/privacy-preserving design: ensuring the privacy-preserving alternatives, like anonymization, local processing on gadgets, and safe compilation, is vital to promoting acceptance and sustaining remarkable security [8], [18].

5.3 Limitations

Several limitations of such a study have cropped up, which should be sorted out in future studies. First, compared to many of the previous studies, the dataset is larger and more heterogeneous and has also been introduced as a limited environment compared to the wide range of behaviours and devices in the real world [8], [20]. The variabilities in the user data, e.g., typing speed degradation during stress or alteration of hand movement patterns, may cause false positives or negatives in case the system fails to accommodate them [4], [20].

Another major difficulty associated with behavioural drift over time is that, as users themselves inevitably change their behavioural patterns, authentication systems might produce erroneous results unless they include methods of updating behavioural profiles without the loss of security [20]. Moreover, the model proved to be robust against simple forms of imitation, but has not been tried out much against intricate forms of spoofing that can involve focused emulation of several behaviour traits as reported in recent adversary analysis [4], [29].

5.4 Future Work

Future directions must concentrate on growing more diverse and larger datasets that cover a wide audience of diverse demographics, devices, and settings to enhance the side of model generalizability [8], [20]. Adding adaptive learning algorithms that can update behavioural profiles throughout an individual would increase resilience to behavioural drift, coupled with a decrease in false rejection [20]. Research on biometrics, including non-behavioural cues, i.e. a combination of behavioural, physiological and contextual attributes, has great potential to reduce vulnerability against advanced attacks [4], [20].

The other important direction is cross-device adaptability, which enables systems to do seamless user authentication on a number of devices with different input qualities. Lastly, further investigation of more advanced adversarial techniques should be conducted to formally assess and improve the system in order to make it robust towards targeted spoofing, securing it in high-stakes setting [4], [29].

6. Conclusion

The paper introduces a continuous authentication system based on Artificial Intelligence: The proposed solution is a system that makes real-time decisions on whether a user is valid or not based on multi-modal behavioural biometrics: keystroke dynamics, mouse movement trajectories, and data provided via motion sensors. It also contributed to high-performance levels compared to regular behavioural biometrics models, with a 97.2% accuracy rate and minimal false rejection and acceptance.

Although this analysis has focused on the practical potential of continuous behavioural authentication to increase security beyond what it is possible under current forms of the static password scheme (and has touched on the need to reserve system adaptability to user behavior variation with time), we may also point out the significance of identifying a practical way of addressing the issues that exist concerning privacy. We used extensive experimentation and analysis of experiments to determine some areas of focus, such as behavioural drift, dataset diversity, or resilience to high-fidelity spoofing training.

Overall, this paper proves that a potential combination of various behavioural modalities and the most modern AI methods can achieve practical, secure, and convenient continuous authentication systems, which will reach the requirements of the current cybersecurity landscape. The future trends in adaptive learning, multi-modality integration, and the availability of technologies to provide privacy-preserving design will be essential in taking such systems out of research and into general use.

References

1. Alquwayzani, A., Aldossri, R., & Frikha, M. (2024). Prominent Security Vulnerabilities in Cloud Computing. *International Journal of Advanced Computer Science and Applications*, *15*(2), 803–813. https://doi.org/10.14569/IJACSA.2024.0150281
2. Abubakar, A. A., Jazim, F., Al-Mamary, Y. H., Abdulrab, M., Abdalraheem, S. G., Siddiqui, M. A., … Alquhaif, A. (2024). Factors influencing students' intention to use learning management system at Saudi Universities: A structural equation modeling approach. *Human Systems Management*, *43*(1), 37–50. https://doi.org/10.3233/HSM-220181
3. Bawitlung, A., Dash, S. K., Lalramhluna, R., & Gelbukh, A. (2024). An Approach to Mizo Language News Classification Using Machine Learning. In *Lecture Notes in Networks and Systems* (Vol. 791, pp. 165–180). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-981-99-6755-1_13
4. Chen, F., Xin, J., & Phoha, V. V. (2024). SSPRA: A Robust Approach to Continuous Authentication Amidst Real-World Adversarial Challenges. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, *6*(2), 245–260. https://doi.org/10.1109/TBIOM.2024.3369590

5. Crocetti, L., Falaschi, F., Saponara, S., & Fanucci, L. (2024). Secure Data Authentication in Space Communications by High-Efficient AES-CMAC Core in Space-Grade FPGA. In *Lecture Notes in Electrical Engineering* (Vol. 1110 LNEE, pp. 49–54). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-031-48121-5_7
6. Doshi, R., & Hiran, K. K. (2024). Explainable artificial intelligence as a cybersecurity aid. In *Advances in Explainable AI Applications for Smart Cities* (pp. 98–113). IGI Global. https://doi.org/10.4018/978-1-6684-6361-1.ch003
7. de Souza, P. R., & Durão, F. A. (2024). Exploiting social capital for improving personalized recommendations in online social networks. *Expert Systems with Applications*, *246*. https://doi.org/10.1016/j.eswa.2023.123098
8. Finnegan, O. L., White, J. W., Armstrong, B., Adams, E. L., Burkart, S., Beets, M. W., … Weaver, R. G. (2024). The utility of behavioral biometrics in user authentication and demographic characteristic detection: a scoping review. *Systematic Reviews*, *13*(1). https://doi.org/10.1186/s13643-024-02451-1
9. Kuang, D., Weng, L., & Kuang, M. (2026). Optimization Management Method of Enterprise Logistics Supply Chain Based on Artificial Intelligence(AI). *International Journal of Computational Systems Engineering*, *10*(1–4). https://doi.org/10.1504/ijcsyse.2026.10062508
10. Kanraweekultana, N., Waijanya, S., Promrit, N., Nopnapaporn, U., Korsanan, A., & Poolphol, S. (2024). Comparison of capability of data classification models to predict consistent results for depression analysis based on user-behaviour tracking and facial expression recognition during PHQ-9 assessment. *Engineering and Applied Science Research*, *51*(1), 11–21. https://doi.org/10.14456/easr.2024.2
11. Kumar, V., Adlin Jebakumari, S., & Meena, M. (2023). Cybersecurity Challenges In Grid-Tied Power Converters. In *2023 International Conference on Power Energy, Environment and Intelligent Control, PEEIC 2023* (pp. 1310–1314). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/PEEIC59336.2023.10450745
12. Khan, M., Nagar, N., Nagpal, M., & Chaudhary, D. (2025). Information Technology Entrepreneurs, Leadership Styles and Employee Engagement: Examining Mediating Effect of Artificial Intelligence. *International Journal of Entrepreneurship and Small Business*, *1*(1). https://doi.org/10.1504/ijesb.2025.10059067
13. Li, M., Banerjee, N. K., & Banerjee, S. (2024). Using Motion Forecasting for Behavior-Based Virtual Reality (VR) Authentication. In *Proceedings - 2024 IEEE International Conference on Artificial Intelligence and eXtended and Virtual Reality, AIxVR 2024* (pp. 31–40). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/AIxVR59861.2024.00012
14. Liu, S., Yang, Z., Liu, S., Liang, R., Sun, J., Li, Q., & Shen, X. (2024). Hyperbolic embedding of discrete evolution graphs for intelligent tutoring systems. *Expert Systems with Applications*, *241*. https://doi.org/10.1016/j.eswa.2023.122451
15. Livingstone, K. M., Rawstorn, J. C., Partridge, S. R., Zhang, Y., Eric, O., Godrich, S. L., … Alston, L. (2024). Determining the feasibility of a codesigned and personalized intervention (Veg4Me) to improve vegetable intake in young adults living in rural Australian communities: Protocol for a randomized controlled trial. *BMJ Open*, *14*(1). https://doi.org/10.1136/bmjopen-2023-078001

16. Murphy, D. P. (2023). Robot and Artificial Intelligence Companies Around the Globe. In *Robotics in Physical Medicine and Rehabilitation* (pp. 33–51). Elsevier. https://doi.org/10.1016/B978-0-323-87865-4.00004-2
17. Miranda-García, A., Rego, A. Z., Pastor-López, I., Sanz, B., Tellaeche, A., Gaviria, J., & Bringas, P. G. (2024). Deep learning applications on cybersecurity: A practical approach. *Neurocomputing*, *563*. https://doi.org/10.1016/j.neucom.2023.126904
18. Md Rasheduzzaman Labu, & Md Fahim Ahammed. (2024). Next-Generation Cyber Threat Detection and Mitigation Strategies: A Focus on Artificial Intelligence and Machine Learning. *Journal of Computer Science and Technology Studies*, *6*(1), 179–188. https://doi.org/10.32996/jcsts.2024.6.1.19
19. Ren, J., Dai, J., & Lin, H. (2024). Simulation of cloth with thickness based on isogeometric continuum elastic model. *Journal of Image and Graphics*, *29*(1), 243–255. https://doi.org/10.11834/jig.221199
20. Sağbaş, E. A., & Ballı, S. (2024). Machine learning-based novel continuous authentication system using soft keyboard typing behavior and motion sensor data. *Neural Computing and Applications*, *36*(10), 5433–5445. https://doi.org/10.1007/s00521-023-09360-9
21. Shareef, O. (2024). Building Organizational Defense: A Comprehensive Approach to Implementing IT Controls for Sox Compliance. *International Journal of Computer Science and Mobile Computing*, *13*(2), 69–71. https://doi.org/10.47760/ijcsmc.2024.v13i02.006
22. Saad, A. M. S. E. (2024). Leveraging Graph Neural Networks for Botnet Detection. In *Communications in Computer and Information Science* (Vol. 1983 CCIS, pp. 135–147). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-031-50920-9_11
23. Sağbaş, E. A., & Ballı, S. (2024). Machine learning-based novel continuous authentication system using soft keyboard typing behavior and motion sensor data. *Neural Computing and Applications*, *36*(10), 5433–5445. https://doi.org/10.1007/s00521-023-09360-9
24. Okada, S., Katano, Y., Kozai, Y., & Mitsunaga, T. (2024). Predicting and Visualizing Lateral Movements Based on ATT&CK and Quantification Theory Type 3. *Journal of Cases on Information Technology*, *26*(1). https://doi.org/10.4018/JCIT.340722
25. Petsani, D., Santonen, T., Merino-Barbancho, B., Epelde, G., Bamidis, P., & Konstantinidis, E. (2024). Categorizing digital data collection and intervention tools in health and wellbeing living lab settings: A modified Delphi study. *International Journal of Medical Informatics*, *185*. https://doi.org/10.1016/j.ijmedinf.2024.105408
26. Vyšniūnas, T., Čeponis, D., Goranin, N., & Čenys, A. (2024). Risk-Based System-Call Sequence Grouping Method for Malware Intrusion Detection. *Electronics (Switzerland)*, *13*(1). https://doi.org/10.3390/electronics13010206
27. Zhang, C., Zhan, D., & Zhao, B. (2026). Using Artificial Intelligence to Construct a Character Expression and Action System for a 3D Human Model. *International Journal of Computational Systems Engineering*, *10*(1–4). https://doi.org/10.1504/ijcsyse.2026.10062235
28. Zhu, W., Zhou, C., & Jiang, L. (2024). A Trusted Internet of Things Access Scheme for Cloud Edge Collaboration. *Electronics (Switzerland)*, *13*(6). https://doi.org/10.3390/electronics13061026

29. Zhao, C., Gao, F., & Shen, Z. (2024). Multi-motion sensor behavior based continuous authentication on smartphones using gated two-tower transformer fusion networks. *Computers and Security*, *139*. https://doi.org/10.1016/j.cose.2023.103698
30. Zhang, Z., Li, H., Hu, H., Chen, T., & Ren, G. (2024). Do non-motorists understand the traffic safety laws protecting them? Results from a Chinese survey. *Travel Behaviour and Society*, *36*. https://doi.org/10.1016/j.tbs.2024.100779