engineering proceedings

MDPI

Proceeding Paper

The Invisible Guardian: Big Data, Behavioral Biometrics, and the Era of Continuous Authentication †

Hadi Fares, Teodora Bakardjieva and Antonina Ivanova *

Department of Computer Science, Varna Free University "Chernorizets Hrabar", 84 Yanko Slavchev Str., Chaika Resort, 9007 Varna, Bulgaria; hadi.fares@vfu.bg (H.F.); bakardjieva@vfu.bg (T.B.)

* Correspondence: antonina.ivanova@vfu.bg

† Presented at the 15th International Scientific Conference TechSys 2026—Engineering, Technologies and Systems, Plovdiv, Bulgaria, 14–16 May 2026.

Abstract

Traditional authentication systems rely mainly on static login checkpoints such as passwords or one-time verification. However, the expansion of cloud services, mobile devices, and distributed digital platforms has exposed significant limitations in these approaches. Modern cyberattacks increasingly exploit credential theft, phishing, and session hijacking in order to bypass login-based security mechanisms. This study examines the use of behavioral biometrics and data-driven analytics in continuous authentication systems that verify user identity throughout an active session. Behavioral interaction signals such as keystroke dynamics, cursor movement patterns, touchscreen gestures, and device usage characteristics can form distinctive behavioral profiles for individual users. Machine-learning models can analyze these signals to detect deviations from established behavioral patterns that may indicate unauthorized access. The paper develops a conceptual framework for continuous behavioral authentication that integrates behavioral monitoring, anomaly detection, and scalable data-processing infrastructures. The analysis highlights both the cybersecurity benefits of behavioral authentication and the challenges related to large-scale behavioral data collection, including privacy protection and responsible data governance.

Keywords: behavioral biometrics; continuous authentication; cybersecurity; big data analytics; machine learning; digital identity

1. Introduction

The expansion of cloud platforms, mobile services, and distributed infrastructures has introduced security challenges that traditional authentication models do not adequately address. Traditional authentication mechanisms based on static credentials such as passwords and one-time verification are increasingly vulnerable to credential theft, phishing attacks, and automated identity fraud. Recent research increasingly focuses on authentication mechanisms that verify identity continuously during user interaction. Finnegan et al. [1] conducted a comprehensive review of behavioral biometrics in authentication systems and highlighted their potential for improving identity verification. The authors demonstrate that interaction-based signals generated during human–computer interaction can serve as distinctive biometric indicators. Their findings emphasize the potential of behavioral biometrics for improving both security and usability in authentication systems. Stylios et al. [2] presented a survey of behavioral biometric techniques used for continuous authentication on mobile devices. The study analyzed multiple behavioral signals, including

Academic Editors: Nikola G. Shakev, Valyo N. Nikolov, Nikolay R. Kakanakov and Sevil A. Ahmed-Shieva

Published: 17 July 2026

keystroke dynamics, touch gestures, and device usage patterns. The authors concluded that combining multiple behavioral features significantly improves authentication accuracy. Baig et al. [3] examined the challenges of implementing continuous authentication systems, focusing on security, usability, and privacy considerations. Their study highlighted the importance of balancing authentication accuracy with user experience. The research also emphasized the need for privacy-preserving techniques when collecting behavioral biometric data. Cheng et al. [4] represent the first trend by combining multiple smartphone-derived signals through optimized ensemble learning, while Mohd Nizam et al. [5] speak to the second by linking touch-stroke authentication with explainable AI. Together, these studies indicate that the field is no longer satisfied with asking whether a model can classify users accurately; researchers are increasingly asking how the decision is made and whether the system can operate in realistic resource conditions.

Verma et al. [6] explored data-driven approaches for behavioral biometric authentication systems. Their research emphasized the role of machine-learning algorithms in analyzing behavioral interaction patterns. The study demonstrated that advanced data analytics techniques can significantly improve authentication reliability.

Uslu et al. [7] investigated the application of deep learning techniques in continuous authentication systems. Their work evaluated several neural network architectures designed to detect behavioral anomalies. The results showed that deep learning approaches can effectively identify complex behavioral patterns. Liebers et al. [8] examined authentication mechanisms based on behavioral biometric signals in digital systems. Their research highlighted the advantages of implicit authentication methods that do not require active user participation. The study suggested that behavioral biometrics can significantly improve security without disrupting user experience. Kang [9] analyzed the role of behavioral biometric authentication in emerging digital environments such as virtual workplaces. The research demonstrated how continuous monitoring of behavioral interaction patterns can enhance security in distributed digital infrastructures. The study emphasized the importance of adaptive authentication frameworks. Zeeshan et al. [10] investigated continuous authentication techniques designed for resource-constrained devices. Their findings demonstrated that behavioral biometrics can be successfully implemented even in environments with limited computational resources. This research highlights the scalability of behavioral authentication models.

Baig et al. [11] further explored privacy-preserving authentication mechanisms for behavioral biometric systems. Their research focused on techniques designed to protect sensitive behavioral data. The authors emphasized the need for secure data management frameworks in behavioral authentication systems. Dillon and De Marsico use keystroke-based continuous assessment in remote examination settings. This application is important for the present article because it illustrates how the same technical logic can be repurposed for educational integrity, not only for enterprise access control. The application of continuous authentication in sensitive environments such as remote examination systems introduces additional governance challenges and requires clear mechanisms for evaluating and contesting automated decisions [12]. Recent studies examine the integration of biometric authentication with decentralized identity infrastructures. The study highlights that combining biometric authentication with decentralized identity architectures may significantly enhance the resilience and scalability of modern digital authentication systems [13].

A growing body of research addresses behavioral biometrics and continuous authentication, with ongoing challenges in integrating behavioral signals into unified cybersecurity architectures. Many existing studies focus on individual behavioral indicators and specific authentication techniques. There is a need for conceptual models that support continu-

ous identity verification across complex digital environments by integrating behavioral micro-gesture analysis with contextual interaction data and adaptive machine-learning mechanisms within scalable security infrastructures.

The present study examines the role of behavioral biometrics and interaction-based identity signals in continuous authentication systems and outlines a conceptual architecture that integrates behavioral monitoring, contextual interaction data, and scalable data-analytics infrastructures. This architecture combines behavioral monitoring, big-data processing, and anomaly detection techniques in order to support adaptive cybersecurity mechanisms capable of identifying suspicious user activity during an active session.

The analysis draws on recent research in behavioral biometrics, user behavior analytics, and data-driven cybersecurity infrastructures and demonstrates how these elements can support scalable continuous authentication systems. The study also introduces the concept of a *digital behavioral rhythm* to describe persistent patterns that emerge from repeated user interaction behavior over time.

The discussion further highlights the importance of balancing adaptive behavioral monitoring with responsible data governance and privacy protection, as large-scale behavioral data collection introduces significant ethical and regulatory considerations.

2. Materials and Methods

This research adopts a conceptual analytical methodology combining literature synthesis with the development of a behavioral continuous authentication framework. The objective is to examine how behavioral interaction signals can support adaptive identity verification systems.

The proposed framework analyzes signals including keystroke dynamics, cursor movement patterns, touchscreen gestures, and device interaction rhythms. These behavioral signals are collected through user devices and processed using machine-learning algorithms capable of constructing behavioral identity profiles.

The architecture assumes the use of distributed big-data infrastructures capable of processing high-velocity interaction streams in real time. Edge computing technologies may also be integrated to reduce latency and minimize centralized storage of sensitive behavioral data.

Figure 1 illustrates the conceptual architecture of the proposed continuous authentication framework based on behavioral biometrics and big data analytics. The model consists of several interconnected layers that enable real-time behavioral identity verification. At the first stage, user interaction sensors embedded in digital devices collect behavioral signals such as keystroke dynamics, cursor movement trajectories, touchscreen gestures, and device usage patterns. These interaction signals are transmitted to a behavioral data processing layer where feature extraction techniques transform raw interaction data into structured behavioral indicators. Machine-learning models then analyze these indicators to construct dynamic behavioral profiles that represent the typical interaction patterns of individual users. The aggregation of these interaction signals over time forms a behavioral pattern referred to in this study as a digital behavioral rhythm, which serves as a reference model for continuous identity verification.

In the next stage, a risk evaluation module continuously compares real-time behavioral signals with the established behavioral profile. When significant deviations from the expected behavioral rhythm are detected, the system generates a risk score that may trigger additional authentication mechanisms, session verification, or security alerts. This layered architecture enables continuous identity verification throughout the entire user session, allowing cybersecurity systems to detect anomalous behavior in real time and respond proactively to potential security threats.

https://doi.org/10.3390/engproc2026150016

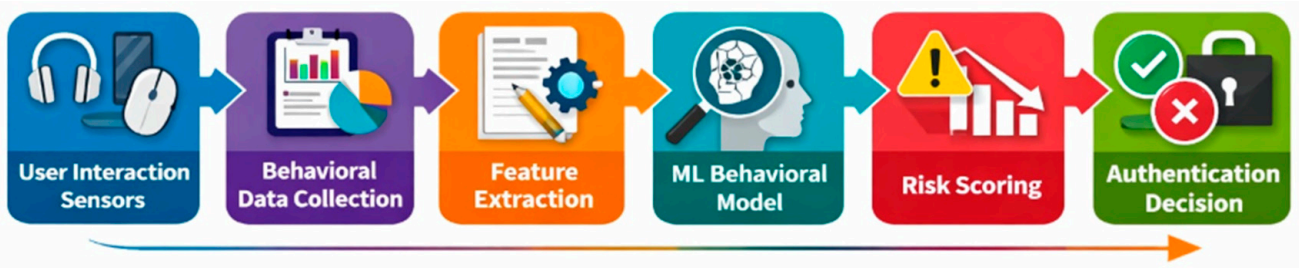

Figure 1. Conceptual architecture of a continuous authentication framework.

Table 1 presents key behavioral biometric techniques used for continuous authentication. The methods differ in the type of behavioral data analyzed, ranging from keystroke dynamics to touchscreen interaction patterns. While these techniques enable passive identity verification, they also introduce limitations related to data variability, hardware differences, and privacy concerns.

Table 1. Behavioral biometric techniques used in continuous authentication.

Technique	Behavioral Data	Advantages	Limitations
Keystroke Dynamics	Typing rhythm	Low-cost implementation	Device variability
Mouse Dynamics	Cursor movement	Passive monitoring	Noise in data
Touch Gestures	Touchscreen interaction	Effective for mobile devices	Hardware differences
Behavioral Profiling	Usage patterns	Continuous monitoring	Privacy concerns

3. Experimental Evaluation

To validate the proposed conceptual framework, an experimental evaluation was conducted using behavioral biometric data representing user interaction patterns. The objective was to assess the effectiveness of continuous authentication based on behavioral signals and anomaly detection techniques.

3.1. Dataset Description

The experiment utilized the CMU Keystroke Dynamics Benchmark Dataset [14], which contains interaction samples collected from 51 users. Each sample includes timing features such as key press duration, latency between keystrokes, and typing rhythm patterns.

To extend the dataset and simulate a more realistic multimodal environment, additional synthetic behavioral features were generated, including mouse movement speed and session activity frequency.

3.2. Experimental Setup

Behavioral features were extracted and normalized before being processed by machine-learning models. The dataset was divided into training (70%) and testing (30%) sets, and model performance was evaluated using cross-validation.

The following models were implemented:

- Random Forest Classifier;
- Support Vector Machine (SVM);
- Long Short-Term Memory (LSTM).

The models were trained to distinguish between:

- Legitimate user behavior;
- Anomalous (unauthorized) behavior.

Evaluation metrics included:

- Accuracy;
- Precision;
- Recall;
- F1-score.

3.3. Results

The experimental results demonstrate that behavioral biometrics can effectively support continuous authentication by enabling accurate discrimination between legitimate and anomalous user behavior. Table 2 presents the quantitative performance of the evaluated machine-learning models based on standard classification metrics, including accuracy, precision, recall, and F1-score. The results indicate consistently high performance across all models, with accuracy values exceeding 90%, which confirms the reliability of behavioral interaction features for identity verification.

Table 2. Performance evaluation of machine-learning models for continuous authentication.

Model	Accuracy	Precision	Recall	F1-Score
Random Forest	94.20%	93.50%	92.80%	93.10%
SVM	91.60%	90.90%	90.20%	90.50%
LSTM	96.80%	96.10%	95.40%	95.70%

Among the evaluated approaches, the LSTM model achieves the highest performance, reaching an accuracy of 96.8% and exhibiting the best results across all evaluation metrics. This performance advantage is related to the model's ability to capture temporal dependencies in behavioral interaction data, which are essential for representing dynamic user activity patterns.

Figure 2 provides a visual representation of model performance across the evaluated metrics. All models demonstrate stable and competitive results. The LSTM model maintains a consistent advantage, particularly in capturing variations in interaction timing and sequence patterns.

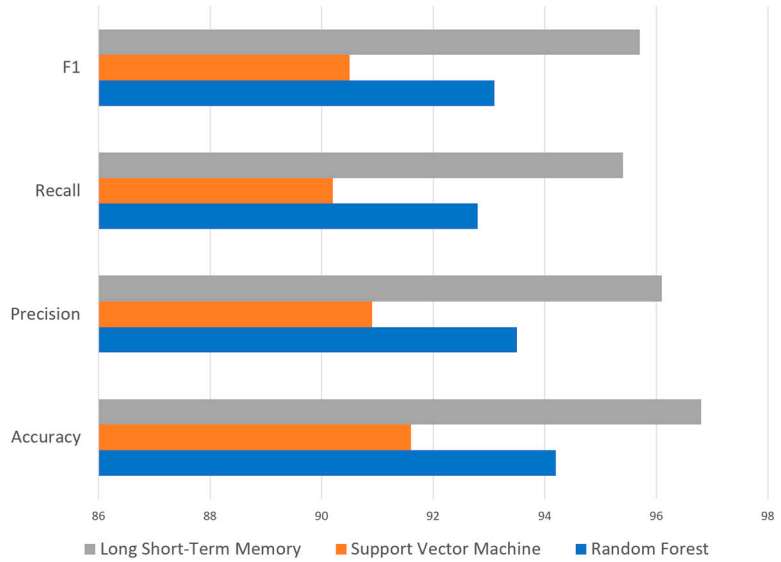

Figure 2. Experimental performance comparison of machine-learning models for behavioral biometric authentication.

https://doi.org/10.3390/engproc2026150016

3.4. Discussion of Results

The findings confirm that continuous authentication based on behavioral biometrics can achieve high accuracy in detecting anomalous user behavior. The integration of multiple behavioral signals improves robustness and reduces false positives.

The results also highlight the importance of temporal modeling in capturing behavioral patterns, supporting the concept of a digital behavioral rhythm introduced in this study.

3.5. Practical Implementation

The proposed framework can be implemented in real-world systems by integrating lightweight behavioral data collectors within user devices, such as web browsers or mobile applications. These collectors capture interaction signals in real time and transmit them to backend processing systems.

Machine-learning models deployed on cloud or edge infrastructures continuously evaluate behavioral patterns and assign risk scores. When anomalies are detected, adaptive responses such as step-up authentication, session termination, or security alerts can be triggered.

Privacy-preserving techniques, including on-device processing and data anonymization, can be applied to ensure compliance with data protection regulations.

4. Findings

Behavioral authentication systems rely on the analysis of subtle interaction patterns generated during user activity. These patterns reflect characteristic features of individual interaction behavior and can serve as behavioral indicators for identity verification. When observed over time, the aggregation of such micro-interaction signals forms what can be described as a digital behavioral rhythm. This concept refers to the temporal and interaction patterns that emerge from repeated human–computer interaction and that characterize the typical activity profile of an individual user. Machine-learning models can analyze these patterns to identify deviations that may indicate unauthorized access attempts or anomalous user behavior.

The integration of contextual signals including device identity, geographic location, and interaction frequency further improves the reliability of behavioral authentication models.

From a big-data perspective, behavioral monitoring generates massive streams of interaction data. Advanced analytics infrastructures are therefore required to process these signals and detect behavioral anomalies across large user populations.

Behavioral authentication changes identity verification from a single login checkpoint to continuous session monitoring. Traditional authentication mechanisms operate on the assumption that identity verification at the login stage is sufficient for maintaining system security. However, modern cyber threats demonstrate that attackers frequently exploit the time interval after authentication, taking advantage of active sessions that remain trusted by the system. Continuous behavioral monitoring addresses this vulnerability by evaluating user interaction patterns throughout the entire session lifecycle, allowing cybersecurity platforms to detect suspicious behavioral deviations in real time.

Behavioral micro-gestures represent an especially valuable source of biometric information because they emerge naturally from human–computer interaction. Subtle characteristics such as typing latency, cursor acceleration, scrolling dynamics, and touchscreen pressure patterns form complex behavioral signatures that are extremely difficult for attackers to replicate accurately. Behavioral micro-gestures such as typing latency, cursor acceleration, and touchscreen pressure patterns can serve as distinctive behavioral indicators that are difficult to imitate consistently. Machine-learning algorithms

trained on such datasets can identify deviations from this rhythm and trigger adaptive authentication responses.

Another important aspect of behavioral authentication is the role of contextual intelligence in improving anomaly detection accuracy. Behavioral patterns rarely exist in isolation; they are influenced by contextual factors such as device type, geographic location, interaction frequency, and time of access. By integrating contextual signals with behavioral micro-gesture analysis, cybersecurity systems can construct multi-dimensional identity profiles that significantly reduce false positives while improving detection of sophisticated attacks. Such hybrid models represent an important step toward the development of adaptive security ecosystems capable of responding dynamically to evolving threat environments.

From a technological perspective, implementing large-scale behavioral authentication requires robust data infrastructures capable of processing massive volumes of interaction data. Large-scale data processing infrastructures enable cybersecurity systems to analyze behavioral interaction signals in real time across large user populations. These infrastructures support the transition from reactive cybersecurity models toward proactive threat detection frameworks in which behavioral anomalies are identified before they escalate into critical security incidents. Consequently, behavioral biometrics may play an important role in future cybersecurity architectures designed for distributed digital environments.

5. Discussion

The proposed framework demonstrates that behavioral biometrics support continuous authentication through interaction-based identity signals. The integration of machine-learning models with behavioral monitoring enables dynamic verification of user identity during active sessions.

Behavioral features such as keystroke dynamics and interaction timing show strong discriminatory capacity for distinguishing legitimate users from anomalous actors. Temporal modeling captures stable interaction patterns, described as a digital behavioral rhythm.

Behavioral patterns evolve over time under the influence of contextual factors, including device characteristics and variations in user interaction. This requires models capable of adaptive learning and periodic updating.

Large-scale deployment raises issues related to data privacy, governance, and computational efficiency. The collection and processing of behavioral data require privacy-preserving methods and clearly defined policies.

The evaluation confirms stable performance under the tested conditions. Further validation with large-scale real-world datasets would support a more complete assessment of robustness and generalizability.

6. Conclusions

The expansion of digital ecosystems has introduced new security risks that traditional authentication models based on static credentials cannot adequately address. Cloud infrastructures, mobile platforms, and globally interconnected information systems operate in environments where identity verification limited to the login stage leaves systems vulnerable to credential theft, phishing attacks, and session hijacking. Continuous authentication based on behavioral biometrics therefore represents an important direction for strengthening adaptive cybersecurity mechanisms. The conceptual framework proposed in this study illustrates how behavioral analytics combined with scalable data-processing infrastructures can support continuous monitoring of user activity and more responsive risk management in complex digital environments.

https://doi.org/10.3390/engproc2026150016

The study examined behavioral authentication systems that rely on interaction signals generated during human–computer interaction. Behavioral indicators such as keystroke dynamics, cursor movement trajectories, touchscreen gestures, and device interaction patterns can form distinctive behavioral signatures that characterize individual users. When analyzed through machine-learning models, these signals allow the construction of behavioral identity profiles capable of detecting anomalous activity during an active session. The concept of a *digital behavioral rhythm* describes how aggregated micro-interaction signals can represent a persistent behavioral identity pattern over time.

Behavioral authentication changes identity verification from a single login checkpoint to continuous session monitoring. Continuous monitoring of interaction patterns enables the detection of suspicious activity and unauthorized access attempts before they escalate into significant security incidents. Such approaches may therefore play an important role in future cybersecurity architectures designed for distributed digital environments.

The implementation of behavioral monitoring technologies raises important ethical and regulatory considerations. Continuous collection of behavioral interaction data introduces challenges related to privacy protection, data governance, and proportional monitoring. The adoption of behavioral authentication systems therefore requires not only technological development but also transparent governance frameworks and responsible management of behavioral data.

Author Contributions: All authors—conceptualization, investigation, data curation, writing—original draft preparation, review and editing, visualization. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The study uses a publicly available dataset and derived behavioral features for experimental evaluation. Processed data are available from the corresponding author upon request.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Finnegan, O.L.; Walsh, D.; Moore, K.; Condell, J. The Utility of Behavioral Biometrics in User Authentication and Identification: A Scoping Review. *Syst. Rev.* **2024**, *13*, 145. [CrossRef] [PubMed]
2. Stylios, I.; Thanou, O.; Androulidakis, I.; Zaitseva, E. Behavioral Biometrics and Continuous User Authentication on Mobile Devices: A Survey. *Comput. Secur.* **2021**, *102*, 102185. [CrossRef]
3. Baig, A.F.; Eskeland, S. Security, Privacy, and Usability in Continuous Authentication Systems. *Sensors* **2021**, *21*, 5967. [CrossRef] [PubMed]
4. Cheng, C.-S.; Chang, K.-C.; Chen, H.-C.; Chou, C.-L. Continuous Smartphone Authentication via Multimodal Biometrics and Optimized Ensemble Learning. *Mathematics* **2026**, *14*, 311. [CrossRef]
5. Mohd Nizam, M.N.; Ooi, S.Y.; Ramalingam, S.; Pang, Y.H. Continuous Authentication through Touch Stroke Analysis with Explainable AI. *Electronics* **2026**, *15*, 542. [CrossRef]
6. Verma, A.; Moghaddam, V.; Anwar, A. Data-Driven Behavioural Biometrics for Continuous and Adaptive User Verification Using Smartphone and Smartwatch. *Sustainability* **2022**, *14*, 7362. [CrossRef]
7. Uslu, U.; Incel, Ö.D.; Alptekin, G.I. Evaluation of Deep Learning Models for Continuous Authentication Using Behavioral Biometrics. *Procedia Comput. Sci.* **2023**, *217*, 1310–1319. [CrossRef]
8. Liebers, J.; Gruenefeld, U.; Buschek, D.; Alt, F.; Schneegass, S. Introduction to Authentication Using Behavioral Biometrics. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems (CHI EA '23)*; Association for Computing Machinery: New York, NY, USA, 2023; pp. 1–4. [CrossRef]
9. Kang, G. Continuous Behavioral Biometric Authentication for Secure Metaverse Offices. *Systems* **2025**, *13*, 588. [CrossRef]

10. Zeeshan, N.; Bakyt, M.; Moradpoor, N.; La Spada, L. Continuous Authentication in Resource-Constrained Devices via Biometric and Environmental Fusion. *Sensors* **2025**, *25*, 5711. [CrossRef] [PubMed]
11. Baig, A.F.; Eskeland, S.; Yang, B. Privacy-Preserving Continuous Authentication Protocols. *Int. J. Inf. Secur.* **2024**, *22*, 1833–1847. [CrossRef]
12. Dillon, R.; De Marsico, M. Behavioral Biometrics for Remote Exam Integrity: Continuous Authenticity Assessment via Keystroke Dynamics. *Procedia Comput. Sci.* **2025**, *274*, 402–411. [CrossRef]
13. Rjab, I.; Sliman, L. Survey on Biometric Authentication for Decentralized Identity Systems. *Future Internet* **2026**, *18*, 126. [CrossRef]
14. Killourhy, K.S.; Maxion, R.A. Comparing anomaly-detection algorithms for keystroke dynamics. In *Proceedings of the 2009 IEEE/IFIP International Conference on Dependable Systems & Networks*; IEEE: New York, NY, USA, 2009; pp. 125–134. [CrossRef]