Volume XXIX 2026
MBNA Publishing House Constanta 2026



Scientific Bulletin of Naval Academy

SBNA PAPER • OPEN ACCESS

Reducing insider threat and human error in maritime operations through continuous behavioral authentication

To cite this article: Sandu Călin, Răcuciu Ciprian, Scientific Bulletin of Naval Academy, Vol. XXIX 2026, pg. 283-288.

Submitted: 29.03.2026
Revised: 28.08.2026
Accepted: 30.09.2026

Available online at www.anmb.ro

ISSN: 2392-8956; ISSN-L: 1454-864X

doi: 10.21279/1454-864X-26-I1-027
SBNA© 2026. This work is licensed under the CC BY-NC-SA 4.0 License

Reducing insider threat and human error in maritime operations through continuous behavioral authentication

Sandu Călin[1*], Răcuciu Ciprian[2]

[1]Școala Doctorală, Academia Tehnică Militară „Ferdinand I", Bucharest, Romania
calin.sandu@yahoo.com
[2]Academia Tehnică Militară „Ferdinand I", Universitatea „Titu Maiorescu"
ciprian.racuciu@gmail.com

Abstract. Maritime digital ecosystems are increasingly composed of interconnected devices and information systems that support navigation, control, communication and operational management. Although access to these systems is typically protected by conventional authentication mechanisms, identity verification occurs only at the beginning of a session. Once access is granted, there is no assurance that the same legitimate operator continues to interact with the system. This limitation creates a significant cybersecurity and safety gap in environments where human interaction with digital equipment has direct operational consequences. This paper explores the concept of continuous behavioral authentication as a complementary cybersecurity layer for maritime operations. Rather than relying solely on static credentials or isolated biometric checks, the proposed approach is based on the continuous analysis of behavioral patterns generated naturally during interaction with digital devices. These patterns (such as keyboard typing rhythm and dynamics, touchscreen pattern usage and motion sensor signals) form a distinctive behavioral profile that can be used to verify operator identity throughout the entire session. The central idea of the paper is the definition of a multi-device behavioral identity model, capable of correlating interaction data collected from different devices within the same operational ecosystem. By treating behavioral interaction as a dynamic identity signal, the approach enables persistent identity verification without interrupting the user's workflow. This conceptual framework aims to reposition behavioral biometrics from a single-device authentication method to a systemic, ecosystem-level identity verification mechanism applicable to safety-critical maritime environments.
Keywords: Cybersecurity, behavioral authentication, multi-device, identity verification, biometrics

1. Introduction

The progressive digitalization of maritime operations has fundamentally transformed how vessels are commanded, monitored, and managed. Modern ships are no longer isolated mechanical platforms; they are networked environments in which bridge navigation systems, engine control interfaces, cargo management terminals, and communication equipment operate as an integrated digital ecosystem. These connected systems span navigation, communication, cargo management, dynamic positioning, terminal management, tracking, and logistics - all increasingly interconnected within the maritime environment. This level of integration, while essential for operational efficiency, introduces significant cybersecurity exposure. The increased connectivity of sensors into command-and-control systems and human-machine interfaces expands the potential cyberattack surface, with risks that include

unauthorized access, data breaches, system manipulation, and the compromise of autonomous systems. The human operator sits at the center of this ecosystem: every interaction with a navigational workstation, an engine monitoring terminal, or a communication panel is a human-machine transaction with direct safety implications.

Conventional authentication mechanisms - typically username/password pairs, PIN codes, or access cards - address the question of identity only at the moment of login. Once access is granted, there is no technical assurance that the authenticated individual remains in control of the session. This architectural gap is particularly consequential in maritime environments, where workstations may be shared across shifts, where physical access to bridge equipment is difficult to control absolutely, and where a compromised or hijacked session could influence vessel trajectory, cargo handling, or emergency response.

This paper investigates keystroke dynamics as a continuous behavioral authentication factor that can operate silently during user interaction with maritime information systems. Unlike static credentials, keystroke patterns form a behavioral biometric signature that can be monitored throughout the entire session without disrupting workflow. The review is positioned within the context of maritime digital ecosystems, with the goal of establishing the conceptual and technical groundwork for a continuous, non-intrusive operator authentication layer applicable to safety-critical shipboard environments. This work is part of a broader research effort aimed at constructing a multi-device behavioral identity model capable of persistent session-level verification across the heterogeneous device landscape found aboard modern vessels.

2. Keystroke dynamics

Keystroke dynamics - also referred to as typing dynamics or typing rhythm biometrics - is the study and application of patterns inherent in an individual's keyboard interaction as a means of identity verification. The main observation is that individuals develop idiosyncratic typing habits through years of keyboard use: the rhythm, force, timing, and sequencing of keystrokes form a behavioral fingerprint that is both distinctive and difficult to consciously replicate. The concept dates to early research in the 1980s, but the field has expanded substantially with the availability of large-scale free-text datasets, machine learning frameworks, and diverse device form factors including touchscreen keyboards.

A fundamental architectural distinction in keystroke-based authentication separates static (fixed-text) from continuous (free-text) approaches. Static verification approaches analyze keystroke characteristics only at specific times - typically during the user login sequence. They provide more robust user verification than simple passwords but make detection of a user change after login impossible. Continuous verification, by contrast, monitors the user's typing behavior throughout the course of the interaction, allowing real-time analysis so that even after a successful login, typing patterns are constantly analyzed and access is blocked when patterns do not match the user's profile. For maritime operational environments, continuous free-text authentication is the only viable paradigm. Operators interacting with workstations, engine control terminals, or communication interfaces do not type predetermined passphrases; they interact with systems using natural, task-driven keystrokes. A system capable of authenticating on this organic input - without interrupting the workflow - constitutes a transparent security layer aligned with operational requirements.

The underlying premise of keystroke biometrics is that typing behavior reflects a combination of cognitive, motor, and habitual factors that are specific to an individual. Neuromotor patterns governing finger movement speed, coordination, and habituation to particular key sequences produce timing signatures that remain substantially consistent within a user over time, while varying meaningfully between users. This stability-versus-distinctiveness balance is what makes keystroke dynamics viable as an authentication signal.

3. Proposed technical implementation

To validate the feasibility of using keystroke dynamics as a continuous authentication signal, a data collection mechanism was implemented in Python.

The script records:

- Key press timestamp
- Key release timestamp
- Inter-key intervals
- Key hold duration
- Long pauses (>1.5 s) as cognitive/behavioral markers

```
if last_press_time:
    interval = press_time - last_press_time
else:
    interval = None

# Detect pause (> 1.5 seconds)
if interval and interval > 1.5:
    keystroke_data.append({
        'key': 'PAUSE',
        'press_time': None,
        'interval': interval,
        'event_type': 'pause',
        'duration': interval
    })
```

Figure 1. Example snippet from the acquisition script

This allows detection of natural cognitive pauses, which are part of the behavioral signature.

```
duration = release_time - press_time

# Add duration to the last press event for this key
for event in reversed(keystroke_data):
    if event['key'] == key_str and event['event_type'] == 'press':
        event['duration'] = duration
        break
```

Figure 2. Recording key hold duration

The resulting dataset is exported for analysis.

```
# Save to CSV file
df = pd.DataFrame(keystroke_data)
df.to_csv('typing_dynamics.csv', index=False)
```

Figure 3. Dataset saved

This dataset forms the basis for behavioral profiling.

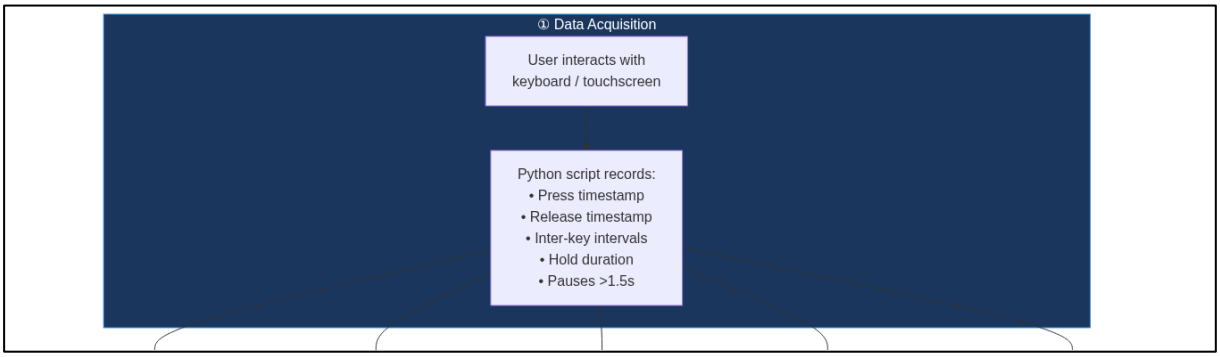
From the raw dataset, the following features can be derived:

Feature	Description	Behavioral Meaning
Inter-key latency	Time between consecutive keys	Typing rhythm
Dwell time	Key press duration	Motor control pattern
Pause frequency	Pauses > 1.5 s	Cognitive pattern
Key usage distribution	Frequency of certain keys	Habitual behavior
Typing speed variance	Stability of rhythm	Fatigue/stress indicator

These features are not static; they evolve during the session and allow continuous identity scoring. Instead of authenticating once, the system continuously computes a behavioral similarity score between:
- The current typing window (e.g., last 30–60 seconds)
- The enrolled behavioral profile of the legitimate operator

If the similarity drops below a threshold, the system can:
- Trigger silent alerts
- Request re-authentication
- Log a potential insider/hijack event

It is important to emphasize that keystroke dynamics represent only one component within a broader research effort, not the final destination of this work. While the present paper focuses on typing rhythm as a proof-of-concept behavioral signal, the research aims to realize a multi-device behavioral authentication layer that integrates input from additional devices such as smartphones or tablets. Extending the proposed model to correlate behavioral profiles seamlessly across multiple devices - accounting for heterogeneous input modalities and contextual variability - remains the central and more ambitious objective of the wider research. Accordingly, the findings reported here serve as foundational groundwork rather than a complete solution.



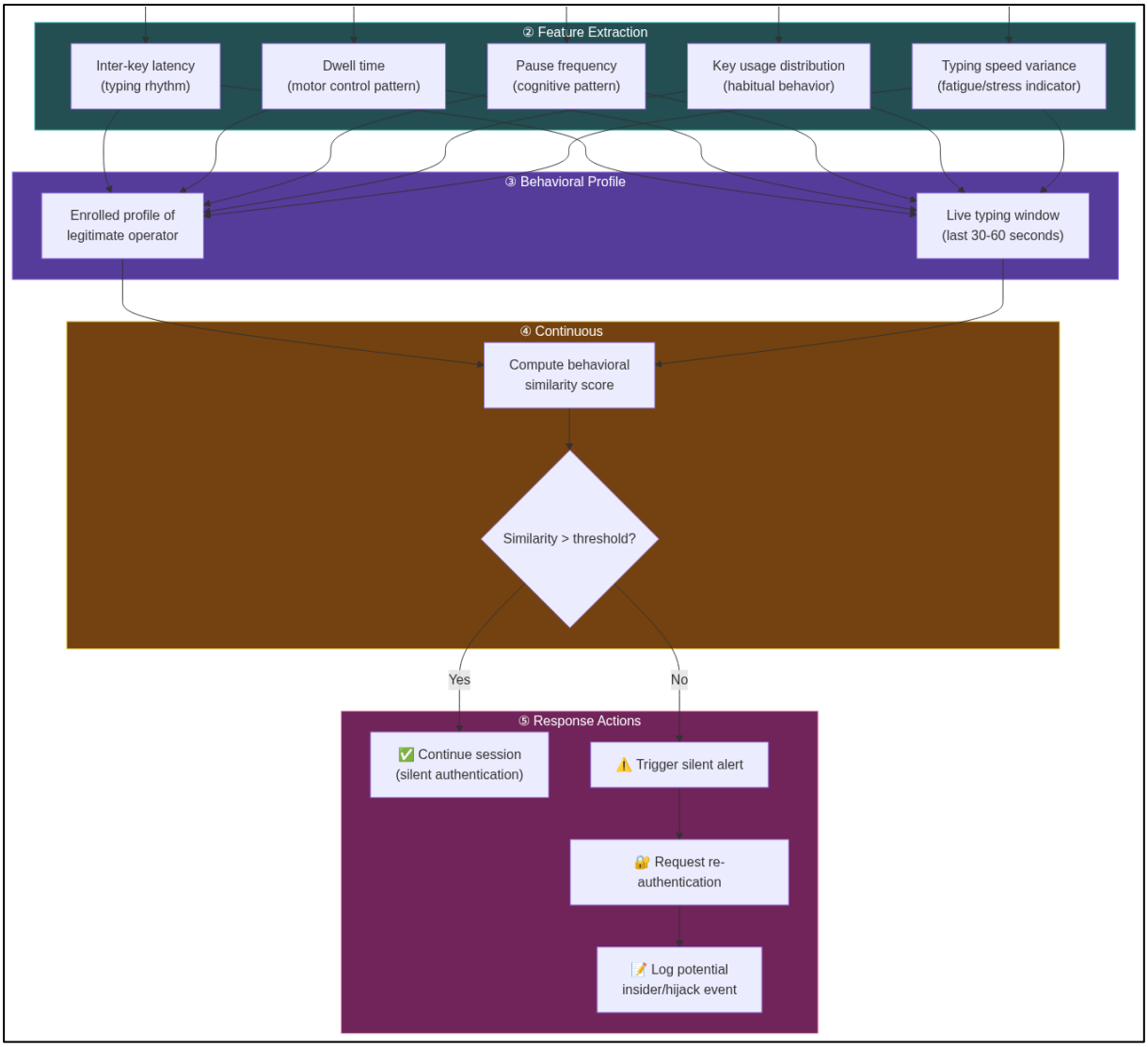


Figure 4. Logical process

Future work will extend the single-device keystroke model to a multi-device behavioral identity framework, integrating input from touchscreens, physical keyboards, and motion sensors (e.g., accelerometer data). Developing methods to correlate behavioral signals across heterogeneous devices without degrading authentication accuracy is a key research direction. Typing patterns may change due to fatigue, stress, seasickness, circadian rhythm shifts, or environmental conditions. Adaptive machine learning models - such as incremental learning or anomaly detection with forgetting mechanisms - are needed to distinguish legitimate behavioral drift from malicious session hijacking.

4. Conclusion

The digital transformation of maritime operations has undeniably enhanced efficiency and connectivity, but it has also introduced critical cybersecurity vulnerabilities. Traditional authentication mechanisms, while effective at the point of login, fail to address the persistent risk of session hijacking or insider threats - risks that are particularly acute in safety-critical environments such as maritime operations. This paper has explored the potential of continuous behavioral authentication, specifically

through the analysis of keystroke dynamics, as a complementary layer to conventional security protocols.

By leveraging the unique behavioral patterns inherent in an operator's interaction with digital systems, continuous authentication offers a non-intrusive, real-time solution to verify identity throughout an entire session. The proposed approach not only mitigates the limitations of static credentials but also aligns with the operational realities of maritime environments, where workflow interruptions are unacceptable and the consequences of unauthorized access can be severe.

The technical implementation demonstrated in the previous section - focusing on keystroke dynamics as a proof-of-concept - highlights the feasibility of extracting and analyzing behavioral features such as inter-key latency, dwell time, and pause frequency. These features form a dynamic behavioral profile that can be continuously compared against live interaction data, enabling the detection of anomalies that may indicate session compromise or insider threats.

However, the research presented here is only a foundational step toward a broader vision: the development of a multi-device behavioral identity framework. Future work must address the challenges of integrating behavioral signals from diverse input modalities - such as touchscreens, physical keyboards, and motion sensors - while accounting for contextual variability and environmental factors like fatigue, stress, or seasickness. Adaptive machine learning models, capable of distinguishing between legitimate behavioral drift and malicious activity, will be essential to ensure the robustness and reliability of such a system.

Continuous behavioral authentication represents a promising paradigm shift in maritime cybersecurity. By treating behavioral interaction as a dynamic identity signal, this approach not only enhances security but also preserves the operational integrity of maritime digital ecosystems. As the research progresses, the integration of multi-device behavioral profiling could set a new standard for identity verification in safety-critical environments, ultimately reducing the risks posed by insider threats and human error in maritime operations.

References

1. R. Shadman, A.A. Wahab, M. Manno, et al., "Keystroke dynamics: concepts, techniques, and applications," arXiv preprint arXiv:2303.04605, 2023.
2. A. Acien, A. Morales, J.V. Monaco, et al., "TypeNet: Deep learning keystroke biometrics," IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 4, no. 1, pp. 57–70, 2022.
3. K. Kanwal, W. Shi, C. Kontovas, et al., "Maritime cybersecurity: are onboard systems ready?" Maritime Policy & Management, 2022.
4. E.A. Sağbaş, S. Ballı, "Machine learning-based novel continuous authentication system using soft keyboard typing behavior and motion sensor data," Neural Computing and Applications, 2024.
5. H.-C. Chang, J. Li, C.-S. Wu, M. Stamp, "Machine learning and deep learning for fixed-text keystroke dynamics," arXiv:2107.00507, 2021.