iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

BEHAVIORAL BIOMETRIC CONTINUOUS USER AUTHENTICATION

Mrs. Bhavana
Assistant Professor, Department of Computer Science and Engineering,
J.B. Institute of Engineering and Technology, Moinabad, Hyderabad, India

Jagati Goutham, Jakkula Karnakar, Javidi Bharath Reddy, and **Nommula Anuroop**
UG Students, Department of Computer Science and Engineering,
J.B. Institute of Engineering and Technology, Moinabad, Hyderabad, India

ABSTRACT
Modern digital systems rely heavily on secure access control, especially in environments where sensitive information is processed. Conventional login-based methods are no longer sufficient because they validate identity only once and can be bypassed through credential compromise or session takeover attacks. This limitation creates a need for mechanisms that can verify user identity continuously during system usage.
The approach presented in this work focuses on evaluating how a user interacts with the system instead of relying only on static credentials. Interaction patterns such as typing rhythm and cursor movement are monitored over time and treated as behavioral signatures. These patterns are analyzed as sequential data, allowing the system to recognize consistency or deviation in user activity.
A sequence-based learning model is used to interpret these interaction streams and generate a confidence measure representing user authenticity. The system operates passively in the background and evaluates data at regular intervals. When a mismatch is detected, an additional verification step is triggered to confirm identity. If the verification fails, access is restricted by ending the active session and limiting application usage. This layered mechanism improves security by combining continuous observation with adaptive decision-making.

INTRODUCTION
Digital applications have become an essential part of everyday activities, particularly in areas such as online transactions, cloud services, and enterprise systems. As these platforms handle critical and sensitive data, ensuring that only authorized users can access them has become a major concern. Most existing systems depend on login-based verification methods, where users are authenticated using credentials like passwords or PINs. Although widely used, these approaches provide only a single checkpoint of validation and are vulnerable to various security threats, including credential leakage, phishing attacks, and unauthorized session access.
A major limitation of these traditional techniques is that they do not verify the user after the login process is completed. Once access is granted, the system assumes that the same user continues to operate the session. This assumption creates a security gap, as an attacker who gains access to valid credentials can continue using the system without further checks. As a result, there is a growing need for authentication mechanisms that operate beyond the initial login stage.
One promising direction involves examining how users interact with a system instead of relying only on what they know. Human interaction patterns—such as typing speed, key transition timing, and mouse movement behavior—tend to be unique and difficult to imitate precisely. These interaction characteristics can serve as a continuous indicator of user identity when monitored over time. Unlike traditional biometrics, this approach does not require specialized hardware and can be implemented using standard input devices.
In this context, the proposed work introduces a monitoring-based authentication framework that evaluates user behavior throughout the active session. The system captures interaction data at regular intervals and analyzes it to determine whether the current activity aligns with previously observed patterns. A sequence-oriented learning model is employed to understand time-based variations in user behavior and identify inconsistencies that may indicate unauthorized usage.
To strengthen decision-making, the system incorporates an additional verification step when irregular behavior is detected. Instead of immediately blocking access, the system requests confirmation from the user, ensuring that temporary variations in behavior do not lead to unnecessary interruptions. This layered approach allows the system to maintain both security and usability.

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

By shifting from single-point verification to continuous evaluation, the proposed method provides a more reliable mechanism for protecting digital sessions. It reduces the risk of unnoticed intrusions and offers a practical solution for environments where maintaining session integrity is critical.

OBJECTIVES

The aim of this work is to design an adaptive authentication approach that strengthens system security by continuously analyzing user interaction behavior. The specific goals of the proposed system are as follows:

1) To establish a mechanism that verifies user identity throughout the active session instead of limiting validation to the initial access stage.
2) To study and utilize interaction-based characteristics, such as typing patterns and cursor activity, as indicators of user identity.
3) To develop a learning-based model capable of interpreting time-dependent behavioral sequences and identifying unusual variations.
4) To minimize the risk of unauthorized usage by detecting inconsistencies in user behavior during ongoing system activity.
5) To implement a background process that gathers and evaluates interaction data without affecting normal user operations.
6) To introduce a confirmation step that is activated only when irregular activity is observed, ensuring both security and usability.
7) To enforce protective actions, including restricting access or ending sessions, when the system identifies potential misuse.
8) To maintain a balance between strong security measures and a smooth user experience by reducing unnecessary interruptions.
9) To enable the system to adjust over time by incorporating updated behavioral patterns for improved accuracy.

SYSTEM DESIGN APPROACH

The system operates through multiple stages, beginning with the collection of user interaction data. A monitoring component captures activities such as typing patterns and cursor movements while the user interacts with the system. This data is gathered continuously without interrupting normal usage.

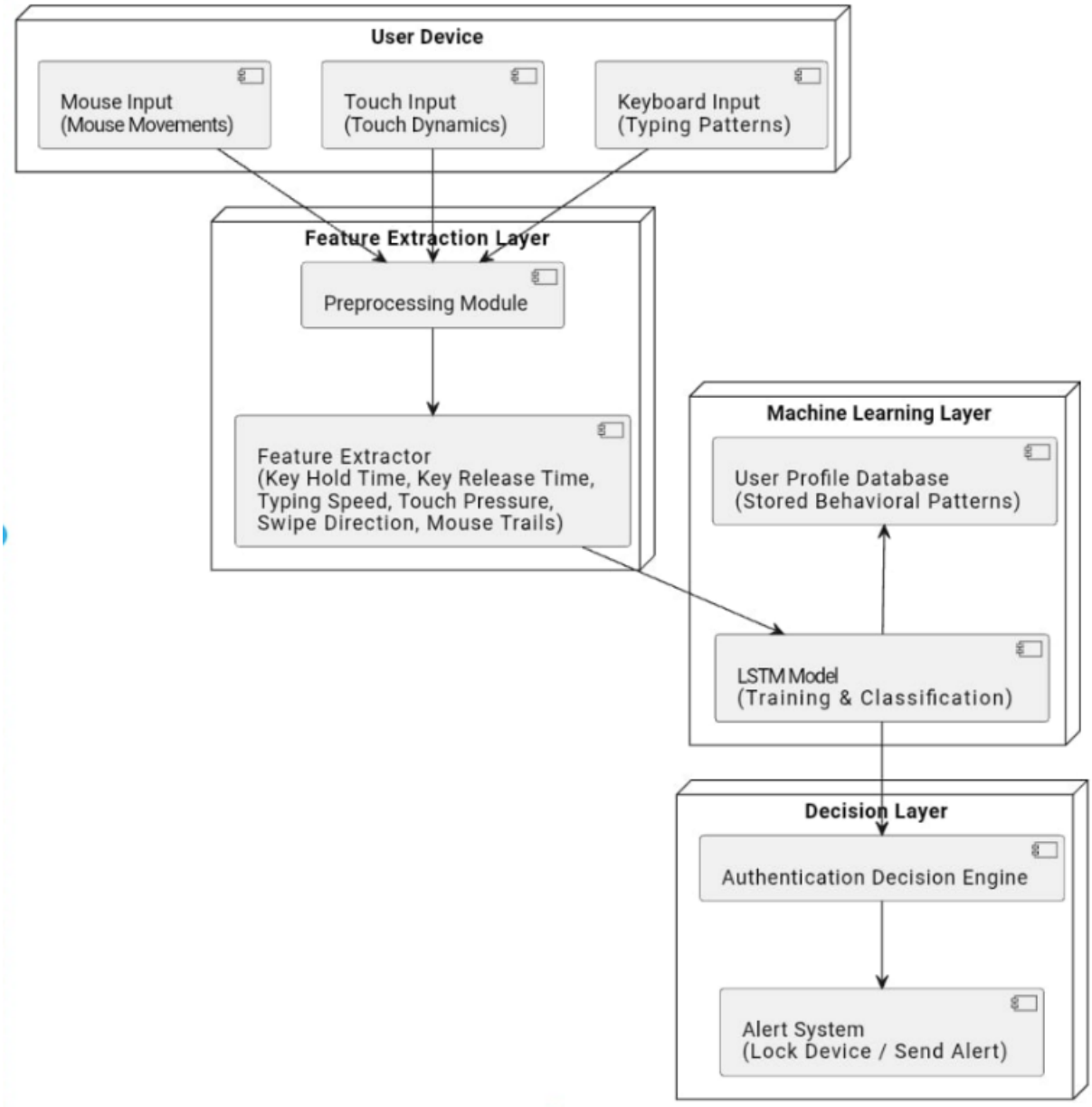
Before analysis, the collected information is refined to remove inconsistencies and prepare it for processing. Relevant behavioral characteristics are then derived from the cleaned data, forming a structured representation of user activity.

A sequential learning model is trained using these behavioral patterns to understand normal user behavior. Once the model is trained, it is used to evaluate real-time data and determine whether the current activity matches the expected pattern.

If a significant difference is detected, the system treats it as a potential security risk. In such cases, an additional confirmation step is triggered to verify the user. Based on the outcome, the system either allows the session to continue or restricts access by ending the session and preventing further interaction.

SYSTEM ARCHITECTURE WORKFLOW

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/



The system architecture for behavioral biometric–based continuous authentication is designed to ensure seamless, real-time monitoring of user interactions to verify identity without interrupting the user experience. It integrates multiple functional layers that work together—starting from raw data collection and processing, followed by intelligent feature extraction, machine learning–based classification, and finally decision-making and alert generation. Each layer plays a crucial role in transforming simple user actions such as typing, touching, or moving the mouse into measurable behavioral patterns that uniquely identify individuals. This layered design enhances security, reduces unauthorized access, and ensures reliable continuous authentication.

PERFORMANCE EVALUATION

The proposed system was tested using behavioral inputs collected from keystroke activity and mouse interactions during normal user sessions. The trained LSTM model was able to learn recurring patterns in user behavior and use them to separate regular activity from suspicious deviations. During evaluation, the model

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

showed stable recognition performance for enrolled users and was able to raise alerts when interaction patterns no longer matched the learned profile. This is consistent with findings in recent continuous-authentication research, where sequence-based models perform well when the input reflects time-dependent behavioral traits.

A key outcome of the implementation was the system's ability to operate continuously rather than only at the login stage. As interaction data was captured in the background, each new batch of behavioral signals was analyzed and assigned a confidence score. When the score remained above the configured threshold, the session proceeded without interruption; when it dropped, the system initiated re-verification. This type of threshold-based decision process is widely used in continuous authentication because it allows the model to respond dynamically to changes in user behavior over time.

The real-time monitoring component functioned effectively during testing. Keystroke timing, mouse speed, click intervals, and cursor path changes were collected at regular intervals and sent to the backend for analysis. The processing time was short enough that the monitoring activity did not noticeably affect normal system usage. This is important because behavioral authentication is only practical if it remains passive and does not interfere with the user's routine workflow.

The OTP-based secondary verification layer added an important safeguard to the overall framework. Instead of terminating a session immediately after one abnormal prediction, the system first requested confirmation from the user through a one-time password. This reduced the chances of unnecessary lockouts caused by temporary behavioral variation, while still preventing unauthorized continuation of the session when verification failed. Similar layered responses are considered useful in continuous authentication because behavioral models may occasionally generate false positives under changing user conditions.

Another useful observation from testing was the effectiveness of application-level enforcement. When the user failed OTP verification, the system closed only the monitored applications rather than shutting down the entire system. This selective response helped maintain security while avoiding unnecessary disruption to unrelated tasks. From a practical standpoint, such a controlled enforcement strategy makes the system more acceptable for real-world deployment, especially in environments where only certain applications handle sensitive information.

At the same time, the evaluation also highlighted a few limitations. Behavioral patterns are not always perfectly stable; typing rhythm and mouse usage can change because of fatigue, stress, injury, or even changes in posture. Research in this area also shows that model performance can vary significantly with feature quality, class imbalance, and threshold sensitivity, which means careful tuning is necessary to reduce both false acceptance and false rejection. As a result, no continuous-authentication model should rely only on raw accuracy; practical deployment requires attention to reliability under realistic usage conditions.

Overall, the results indicate that the proposed approach is suitable for strengthening session security beyond traditional login-based authentication. By combining behavioral monitoring, LSTM-based sequence analysis, OTP re-verification, and controlled application shutdown, the system creates multiple layers of defense against session misuse. The discussion also suggests that future improvement should focus on collecting richer behavioral samples, reducing false alarms, and adapting the model to natural changes in user behavior over time.

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to their guide and faculty members of the Department of Computer Science and Engineering, J.B. Institute of Engineering and Technology, for their continuous support, valuable suggestions, and encouragement during the course of this work. Their guidance played an important role in shaping the technical direction and completion of the project.

The authors also thank the department and institution for providing the academic environment, laboratory facilities, and resources needed to carry out this research successfully. Appreciation is extended to friends and classmates who offered useful feedback and motivation at different stages of the project.

Finally, the authors are deeply thankful to their parents and family members for their patience, moral support, and confidence throughout the development of this paper. Their encouragement remained a constant source of strength during the entire research process.

CONCLUSION

This work presents a continuous authentication approach that strengthens session security by moving beyond one-time login verification. By observing keystroke behavior and mouse interaction patterns throughout active usage, the system can evaluate whether the current user still matches the enrolled profile. The use of an LSTM model makes the framework suitable for learning time-dependent behavioral patterns and identifying deviations

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

that may indicate unauthorized access. Research in this area similarly recognizes sequential behavioral analysis as a practical direction for improving real-time authentication.

An important contribution of the proposed system is the combination of behavioral monitoring with OTP-based re-verification and controlled application shutdown. This layered response improves security because it does not rely on a single decision point; instead, it verifies suspicious activity before enforcing session termination. Such continuous and adaptive validation is closely aligned with Zero Trust thinking, where access is treated as something that must be checked repeatedly rather than assumed after login.

At the same time, the study also shows that continuous authentication systems must handle real-world variability in user behavior. Factors such as fatigue, stress, device usage conditions, and long-term habit changes can influence model predictions and may increase false alerts if the system is not tuned carefully. Existing research also highlights the importance of larger datasets, multimodal signals, and adaptive learning to make these systems more stable and practical for deployment.

Overall, the proposed framework offers a useful and scalable direction for protecting sensitive digital sessions in domains such as banking, enterprise platforms, and secure web applications. Future improvements can focus on richer behavioral feature collection, stronger resistance to spoofing, privacy-aware data handling, and models that update with gradual user behavior changes over time. These enhancements would make the system more reliable and better suited for real-world cybersecurity environments.

REFERENCES

1) [1] F. Monrose and A. D. Rubin, "Keystroke dynamics as a biometric for authentication," Future Generation Computer Systems, vol. 16, no. 4, pp. 351–359, 2000. [ppl-ai-file-upload.s3.amazonaws](https://ppl-ai-file-upload.s3.amazonaws.com/web/direct-files/attachments/87364423/abe88443-abc0-4c51-a089-0a51a1d3b28e/IJETRM_ADR_DDI-major-project.doc)
2) [2] K. S. Killourhy and R. A. Maxion, "Comparing anomaly-detection algorithms for keystroke dynamics," in Proceedings of the IEEE/IFIP International Conference on Dependable Systems & Networks, 2009, pp. 125–134. [ijcaonline](https://www.ijcaonline.org/archives/volume187/number5/lstm-based-free-text-keystroke-dynamics-for-continuous-authentication/)
3) [3] S. Hochreiter and J. Schmidhuber, "Long short-term memory," Neural Computation, vol. 9, no. 8, pp. 1735–1780, 1997. [dl.acm](https://dl.acm.org/doi/10.1145/3052973.3053032)
4) [4] M. Eberz, K. B. Rasmussen, V. Lenders, and I. Martinovic, "Evaluating behavioral biometrics for continuous authentication: Challenges and metrics," in Proceedings of the ACM Conference on Computer and Communications Security, 2017, pp. 386–399. [arxiv](https://arxiv.org/html/2210.16819v3)
5) [5] E. Giot, M. El-Abed, and C. Rosenberger, "Keystroke dynamics authentication for collaborative systems," in Proceedings of the IEEE International Conference on Collaborative Computing, 2011, pp. 172–179. [jatit](https://www.jatit.org/volumes/Vol103No2/10Vol103No2.pdf)
6) [6] S. Banerjee and D. Woodard, "Biometric authentication and identification using keystroke dynamics: A survey," Journal of Pattern Recognition Research, vol. 7, no. 1, pp. 116–139, 2012. [ijcaonline](https://www.ijcaonline.org/archives/volume187/number5/azanguezet-2025-ijca-924780.pdf)
7) [7] Y. Meng, D. Wong, R. Schlegel, and L. Kwok, "Touch gestures based biometric authentication scheme for mobile devices," Information Forensics and Security, vol. 8, no. 11, pp. 1860–1873, 2013. [jetir](https://www.jetir.org/papers/JETIR2511616.pdf)
8) [8] A. Ahmed and I. Traore, "A new biometric technology based on mouse dynamics," IEEE Transactions on Dependable and Secure Computing, vol. 4, no. 3, pp. 165–179, 2007. [nature](https://www.nature.com/articles/s41598-025-14833-z)
9) [9] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016. [journal.paluniv.edu](https://journal.paluniv.edu.ps/index.php/ajbte/article/download/144/208/297)
10) [10] N. Patel, R. Shah, and P. Patel, "AI-based continuous authentication system using behavioral biometrics," International Journal of Computer Applications, vol. 183, no. 25, pp. 1–6, 2021. [diva-portal](https://www.diva-portal.org/smash/get/diva2:2001372/FULLTEXT01.pdf)