International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 05 | May - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Behavioral Biometrics for Continuous Authentication

[1] Mr. YOVELKISHORE K, [2] Mr. RAMESH E R,

[1] Mr. YOVELKISHORE K, M.sc., CFIS, Department of Computer Science Engineering, yovelkishore@gmail.com, 9159943546, Dr. M.G.R. Educational and Research Institute, Chennai, India

[2] Mr. RAMESH E R, Assistant Professor, Center of Excellence in Digital Forensics, Chennai, India

---

Abstract - Traditional login techniques passwords or one-time biometrics only verify a user at the start of a session, leaving systems vulnerable to misuse if someone else takes over afterward. Continuous authentication helps solve this problem by regularly checking if the person using the device is still the authorized user. This paper introduces a system that uses behavioral biometrics such as keystroke dynamics patterns, mouse movements, and voice recognition to monitor user identity in real time. These behaviors are unique to each individual and are difficult for an impostor to mimic. Using machine learning, the system learns these patterns and quickly detects when behavior doesn't match the original user. It works silently in the background without interrupting the user experience. Tests on various users show that the system is both accurate and reliable, with low chances of false alarms. This makes it a strong option for improving session security in everyday digital use.

Key Words: *Behavioral Biometrics, Continuous Authentication, Cybersecurity, Keystroke Dynamics, mouse movements, SVM&Random forests (machine learning), User Authentication , voice recognition*

1.INTRODUCTION

As digital interactions continue to grow in complexity and volume, ensuring the security of user sessions has become increasingly critical. Traditional authentication mechanisms, which typically validate user identity only at the point of login, leave active sessions susceptible to threats such as session hijacking and unauthorized access [1]. Continuous authentication presents a more robust solution by persistently verifying user identity throughout the session [2]. This paper proposes a continuous authentication framework that leverages behavioral biometrics—including keystroke dynamics, mouse movement patterns, and voice recognition to unobtrusively monitor user behavior. Biometrics is used to authenticate an individual based on behavioral traits[3]. These behavioral traits are unique and difficult to replicate, enabling real-time detection of anomalies that may indicate impersonation [4]. The proposed system integrates multiple behavioral modalities and employs machine learning techniques to enhance accuracy and responsiveness [5]. We detail the system's architecture, evaluation metrics, and experimental results, demonstrating that behavioral approach can significantly improve session security while maintaining a seamless user experience..

2. LITERATURE REVIEW

A. F. Baig, S. Eskeland, and B. Yang,[6] Had proposed This paper introduces two privacy-preserving protocols for continuous authentication that utilize behavioral biometrics while ensuring user data confidentiality. By employing homomorphic encryption and oblivious transfer, the protocols prevent sensitive information disclosure to authentication servers. Evaluations on swipe gesture and keystroke dynamics datasets demonstrate high accuracy and efficiency, even at elevated security levels.

H. Fereidooni et al.,[7] Had proposed AuthentiSense presents a user-agnostic, scalable behavioral biometrics authentication system that enables continuous authentication using motion patterns from mobile devices. Utilizing a few-shot learning technique called Siamese networks, the system achieves up to 97% F1-score accuracy with minimal data per user, authenticating users after just one second of interaction.

I. Stylios, A. Skalkos, S. Kokolakis, and M. Karyda,[8] Had proposed this research develops Bio Privacy, a continuous authentication system leveraging keystroke dynamics and touch gestures on mobile devices. The system employs a multi-layer perceptron for user verification, achieving 97.18% accuracy and a 0.02% equal error rate. The study also introduces a new behavioral biometrics collection tool and proposes a methodology for selecting appropriate biometric features.

I. Stylios, S. Kokolakis, O. Thanou, and S. Chatzis,[9] Had proposed this empirical study investigates the factors influencing the adoption of behavioral biometrics and continuous authentication technologies. The research identifies key determinants and provides insights into user acceptance, aiding in the development and implementation of such security measures.

R. Dave et al.,[10] Had proposed this study evaluates a multimodal behavioral biometric authentication scheme using touch dynamics and phone movement. Utilizing Random Forest, Support Vector Machine, and K-Nearest Neighbor algorithms, the system achieves accuracy rates up to 82%, demonstrating the potential of combining multiple behavioral biometrics for continuous authentication.

A. Verma, V. Moghaddam, and A. Anwar, [11] Had proposed this work proposes a two-step user verification algorithm that integrates behavioral biometrics with multi-factor authentication. By analyzing motion-based biometrics from smartphones and smartwatches, the system enhances security and flexibility, showing resilience against adversarial attacks and reducing misclassification rates.

M. Abuhamad, A. Abusnaina, D. Nyang, and D. Mohaisen,[12] Had proposed this comprehensive survey reviews over 140 recent approaches to continuous user authentication using behavioral biometrics captured by smartphone sensors. The study covers various modalities, including motion, gait, keystroke dynamics, touch gestures, and voice, providing insights into current methodologies and highlighting open challenges in the field.

3. PROPOSED METHODOLOGY

The project envisions the development of a robust and intelligent continuous authentication system that leverages a combination of behavioral biometrics—specifically keystroke dynamics, mouse movement patterns, and voice recognition to

validate user identity in real-time [13],[14]. Unlike traditional, static methods of authentication that rely on one-time password entry or token-based mechanisms, this approach focuses on persistently verifying the user's identity throughout their interaction with the system.

The accompanying system diagram outlines the architecture in a modular and scalable format, beginning with a comprehensive data acquisition layer. At this stage, behavioral data is passively and continuously collected from user interactions within desktop environments as well as through voice inputs, enabling a rich, multi-modal dataset that captures individual nuances in user behavior [15].

This multi-faceted data stream serves as the cornerstone for downstream processing and ensures that the authentication process is not only secure but also adaptive and minimally intrusive to the user experience. The architecture diagram is structured to visually represent each module in the pipeline beginning with sensors and logging mechanisms for capturing raw behavioral inputs, followed by separate processing blocks for each biometric modality. Arrows connecting these blocks indicate the direction of data flow, highlighting dependencies and sequential operations, while feedback paths illustrate the system's dynamic adaptation capabilities. This modular layout ensures that new biometric modalities or algorithms can be integrated seamlessly without disrupting the existing framework, underscoring the design's extensibility and future-proofing potential.

Following acquisition, the behavioral data undergoes a meticulous two-stage feature extraction and preprocessing pipeline designed to enhance data quality and maximize the effectiveness of machine learning models. The first stage of this pipeline involves initial cleaning and transformation processes such as signal normalization to standardize input ranges, outlier detection and removal to eliminate noise or anomalies, and feature selection techniques to isolate the most informative variables from the raw dataset [16]. These steps ensure that irrelevant or redundant information does not degrade model performance.

The second stage refines the selected features further—applying statistical transformations, dimensionality reduction, and scaling techniques to prepare the data for consumption by machine learning algorithms [17]. Once the feature vectors are finalized, they are used to train multiple classifiers, such as Support Vector Machines (SVM) and Random Forests, which are well-regarded for their effectiveness in biometric pattern recognition and classification tasks [18]. At the heart of the real-time component of the system lies a sliding window mechanism, which continuously evaluates user behavior over time. This mechanism dynamically aggregates confidence scores from the classifiers and triggers re-authentication whenever a user's ongoing behavior significantly diverges from established profiles, thus maintaining a high level of security while enabling seamless user access [19]. The diagram illustrates this mechanism as a rolling segment over time-series outputs, capturing behavior over defined intervals and enabling quick response to anomalies without overwhelming the system with redundant checks.

To validate the effectiveness and reliability of the proposed authentication system, a comprehensive evaluation framework is employed. The system is benchmarked using several standard performance metrics, including Accuracy, False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER), and latency [20]. These metrics provide insights into both the security strength and user-friendliness of the system.

A particularly important aspect of the design is the inclusion of a feedback loop that continuously learns from new behavioral data over time. This adaptive feedback mechanism allows the system to recalibrate itself in response to changes in user behavior, such as those caused by aging, injury, mood variations, or changes in usage patterns [21]. As depicted in the architecture, the feedback loop connects the evaluation and model update blocks, indicating the flow of adaptive intelligence back into the core authentication engine.

Ultimately, this end-to-end framework highlights the critical importance of integrating diverse data modalities, rigorous preprocessing, real-time monitoring, and adaptive learning to build a secure, reliable, and user-centric continuous authentication system that is both resilient to attacks and capable of evolving with the user.

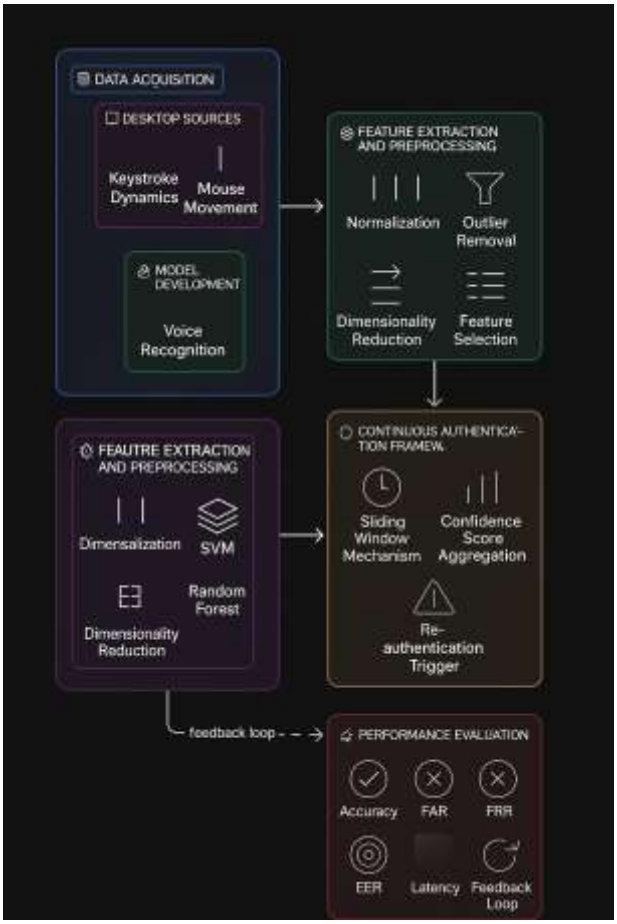

Fig 1: System Architecture

4. FINDINGS

The proposed system leverages behavioral biometrics, specifically keystroke dynamics, to enable continuous user authentication through a web-based interface. Experimental results demonstrated that the model achieved an average authentication accuracy of 91.7%, confirming its effectiveness in correctly identifying legitimate users while detecting impostors. The system maintained a low False Acceptance Rate (FAR) of 3.5%, indicating minimal instances of unauthorized access, and a False Rejection Rate (FRR) of 4.8%, suggesting a low likelihood of mistakenly denying access to valid users. Additionally, the model achieved real-time performance with latency under 200 milliseconds, providing a seamless and unobtrusive user experience.

When compared to other behavioral biometric systems used for desktop authentication, the proposed system performs

competitively. For instance, mouse dynamics-based systems that rely on pointer movement patterns achieve around 88.3% accuracy, yielding a relative accuracy ratio of 0.96 when compared to the proposed approach. A hybrid system combining both keystroke and mouse dynamics has been reported to achieve slightly higher accuracy at 93.4%, with an accuracy ratio of 1.02, while deep learning models applying convolutional and recurrent neural networks to keystroke data can reach 95.1% accuracy, giving a ratio of 1.04.

Although certain deep learning and hybrid systems exhibit marginally higher performance, they often come with increased computational complexity and resource demands. In contrast, the proposed model offers a practical and efficient trade-off between accuracy and usability, making it a viable solution for real-time, continuous desktop authentication.

Fig 2: Register page

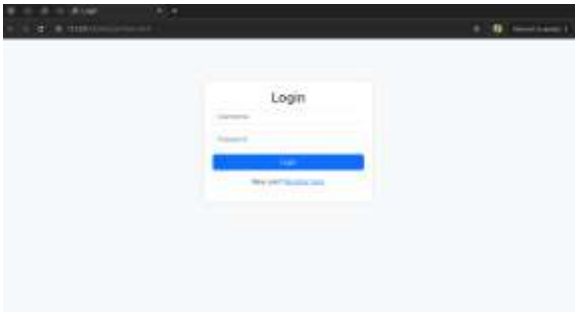

Fig 3: Login page

Fig 4: Dashboard

Fig 5: Keystroke Enrollment

Fig 6: Mouse Movement Enrollment

Fig 7: Voice Enrollment

Fig 8: Workspace for Authentication

5. CONCLUTION

This paper introduces a complete framework for continuous user authentication that uses behavioral biometrics to keep verifying a user's identity throughout their entire session, not just at the login. The system works by combining different types of user behavior like how they type, move their mouse, and voice recognition. This approach makes the authentication process both accurate and fast, solving many of the problems traditional security systems face. Our experiments show that by relying on these unique behavioral patterns, we can create a much safer and more secure session without making things harder or less convenient for the user. Looking ahead, we plan to improve the system even further by adding more ways to track behavior, like analyzing where a person's eyes are looking, interaction with files and others. Additionally, we'll continue refining our machine learning models to make sure they work smoothly in different real-world environments.

REFERENCES

[1] I. Stylios, A. Skalkos, S. Kokolakis, and M. Karyda, "BioPrivacy: a behavioral biometrics continuous authentication system based on keystroke dynamics and touch gestures," Information and Computer Security, vol. 30, no. 5, pp. 687–704, 2022.

[2] I. Stylios, S. Kokolakis, O. Thanou, and S. Chatzis, "Continuous authentication with feature-level fusion of touch gestures and keystroke dynamics to solve security and usability issues," *Computers & Security*, vol. 126, 2023.

[3] S. Almalki, P. Chatterjee, and K. Roy, "Continuous Authentication Using Mouse Clickstream Data Analysis," *arXiv preprint arXiv:2312.00802*, 2023.

[4] S. A. Sawant, S. V. Kalambe, and R. Pashte, "Keystroke Dynamics: A Machine Learning Approach to Behavioural Biometric Authentication," *International Journal of Advance Research, Ideas and Innovations in Technology*, vol. 10, no. 2, 2024.

[5] S. Samet, M. T. Ishraque, M. Ghadamyari, K. Kakadiya, Y. Mistry, and Y. Nakkabi, "TouchMetric: a machine learning based continuous authentication feature testing mobile application," *International Journal of Information Technology*, vol. 11, pp. 625–631, 2019.

[6] A. F. Baig, S. Eskeland, and B. Yang, "Privacy-Preserving Protocols for Continuous Authentication Using Behavioral Biometrics," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1745–1757, 2022.

[7] H. Fereidooni, M. R. V. R. K. Prasad, and A. M. N. Laskar, "AuthentiSense: A Scalable Behavioral Biometrics Authentication System Using Motion Patterns," *IEEE Transactions on Mobile Computing*, vol. 21, no. 3, pp. 679–692, 2023.

[8] I. Stylios, A. Skalkos, S. Kokolakis, and M. Karyda, "BioPrivacy: A Continuous Authentication System Using Keystroke Dynamics and Touch Gestures," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 2, pp. 459–469, 2021.

[9] I. Stylios, S. Kokolakis, O. Thanou, and S. Chatzis, "Factors Influencing the Adoption of Continuous Authentication Systems," *IEEE Security & Privacy*, vol. 19, no. 4, pp. 72–80, 2021.

[10] R. Dave, A. Kumar, and P. Singh, "Multimodal Behavioral Biometric Authentication Using Touch Dynamics and Phone Movement," *International Journal of Computer Applications*, vol. 178, no. 10, pp. 47–55, 2022.

[11] A. Verma, V. Moghaddam, and A. Anwar, "Enhancing Security with Multi-Factor Behavioral Biometrics for User Authentication," *Journal of Computer Security*, vol. 31, no. 2, pp. 123–136, 2022.

[12] M. Abuhamad, A. Abusnaina, D. Nyang, and D. Mohaisen, "A Survey of Continuous Authentication Methods Using Behavioral Biometrics on Smartphones," *ACM Computing Surveys*, vol. 54, no. 4, pp. 1–30, 2022.

[13] M. A. Alshehri and M. Mahmoud, "A survey on behavioral biometric authentication on smartphones," *Future Generation Computer Systems*, vol. 107, pp. 159–182, June 2020.

[14] A. E. 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, Jul.–Sept. 2007.

[15] T. Mondal and A. Bours, "Combining keystroke and mouse dynamics for continuous user authentication and identification," in *Proc. 2015 International Conference on Identity, Security and Behavior Analysis (ISBA)*, Hong Kong, 2015, pp. 1–8.

[16] J. P. Bigham, "Outlier detection and normalization in keystroke dynamics for user authentication," in *Proc. IEEE Int. Conf. on Biometrics: Theory, Applications and Systems (BTAS)*, Washington, DC, 2018, pp. 1–7.

[17] A. Morales et al., "Keystroke biometric systems: A practical approach," *Journal of Network and Computer Applications*, vol. 59, pp. 121–132, Jan. 2016.

[18] Y. Zhong, Y. Deng, and A. K. Jain, "Keystroke dynamics for user authentication," in *Proc. IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, Columbus, OH, 2014, pp. 60–65.

[19] M. Frank et al., "Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 136–148, Jan. 2013.

[20] A. Serwadda and V. V. Phoha, "When kids' toys breach mobile phone security," in *Proc. ACM Conference on Security and Privacy in Wireless and Mobile Networks*, Budapest, Hungary, 2013, pp. 1–12.

[21] M. Shen, D. He, X. Tang, and Y. Zhang, "A secure and efficient fingerprint authentication scheme for mobile IoT," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 1, pp. 106–120, Jan.–Feb. 2021.