International Journal of Electrical, Electronics and Computer Systems

ISSN: 2347-2820

Volume 15 Issue 01 (2026) | Pages: 100-103

Result Paper on Mouse Dynamics Based Bot Detection System

G.G. Sayyed[1], Sahil Kadam[2], Saneel Gogade[3], Kishor Kadam[4], Ritesh Zagade[5]

[1,2,3,4,5]S.B. Patil College of Engineering, Indapur

[2]*sahilgkadam19@gmail.com*, [3]*saneelgodage@gmail.com*, [4]*kishorkadam1817@gmail.com*, [5]*zagaderitesh2113@gmail.com*

Peer Review Information

***Type**: Article*
***Received**: 24 March 2026*
***Revised**: 09 April 2026*
***Accepted**: 27 May 2026*
***Published**: 06 June 2026*

Abstract

With the increasing number of automated attacks on web applications, traditional security mechanisms are becoming insufficient. Bots can bypass CAPTCHA and mimic human-like interactions, making detection challenging. This project proposes a Mouse Dynamics Based Bot Detection System to distinguish human users from automated scripts. The system captures real-time mouse movement data such as position, velocity, and acceleration. Behavioral features are extracted and analyzed using machine learning techniques. The system evaluates patterns like movement randomness, speed variation, and interaction duration. A web-based interface integrates data collection and real-time prediction. The system provides immediate classification results with confidence scores. It enhances security by identifying abnormal interaction patterns. The approach is lightweight and does not interrupt user experience. Overall, it improves authentication systems by adding behavioral biometrics.

Keywords: Mouse Dynamics; Bot Detection; Machine Learning; Behavioral Biometrics; Cybersecurity.

How to Cite This Article

Sayyed, G. G., Kadam, S., Gogade, S., Kadam, K., & Zagade, R. (2026). Result paper on mouse dynamics based bot detection system. *International Journal of Electrical, Electronics and Computer Systems*, 15(1), 100–103.

Introduction

Web applications are increasingly targeted by automated bots. These bots perform malicious activities such as credential stuffing and spam attacks. Traditional security methods like passwords and CAPTCHA are no longer fully reliable. Bots have evolved to mimic human behavior. This creates a need for advanced detection mechanisms. Behavioral biometrics provides a promising solution. Mouse dynamics is a unique behavioral pattern of each user. It includes speed, direction, and movement style. Humans show irregular and natural movements. Bots typically follow predictable or overly smooth patterns. Analyzing these differences helps in detection. The system collects real-time mouse movement data. It processes features such as velocity and acceleration. Machine learning models classify behavior. The system works in real-time. It integrates seamlessly with login systems. No additional effort is required from users. This improves both security and user experience. It reduces reliance on traditional authentication methods. The system is scalable and efficient. It can be deployed across multiple applications. Overall, it strengthens cybersecurity defenses.

Literature Survey

Research in behavioral biometrics has grown rapidly. Mouse dynamics has been widely studied for authentication. Machine learning models such as Random Forest and SVM are commonly used. Velocity and acceleration features are key indicators. Some systems use keystroke dynamics along with mouse data. However, many systems lack real-time implementation. Few provide integration with web interfaces. Most studies focus only on offline datasets. Real-time detection systems are limited.

Research Gap

Existing systems lack real-time detection capabilities. Most research uses static datasets. Integration with live web applications is limited. Bot simulation techniques are not realistic. Detection accuracy varies across environments. Systems often fail against advanced bots. Feature extraction is sometimes incomplete. User experience is not prioritized. There is limited visualization of results. Scalability is not properly addressed. Many models are computationally heavy. There is lack of controlled demo environments. Security validation is insufficient. Dataset diversity is limited. System reliability is not guaranteed. This project addresses these gaps.

Problem Statement

Web applications face increasing bot attacks. Traditional authentication methods are insufficient. Bots can mimic human behavior effectively. There is no reliable real-time detection system. User experience should not be affected. The system must detect bots accurately. It should work with live web interaction. It must process data efficiently. The solution should be scalable. An intelligent behavioral detection system is required.

System Architecture

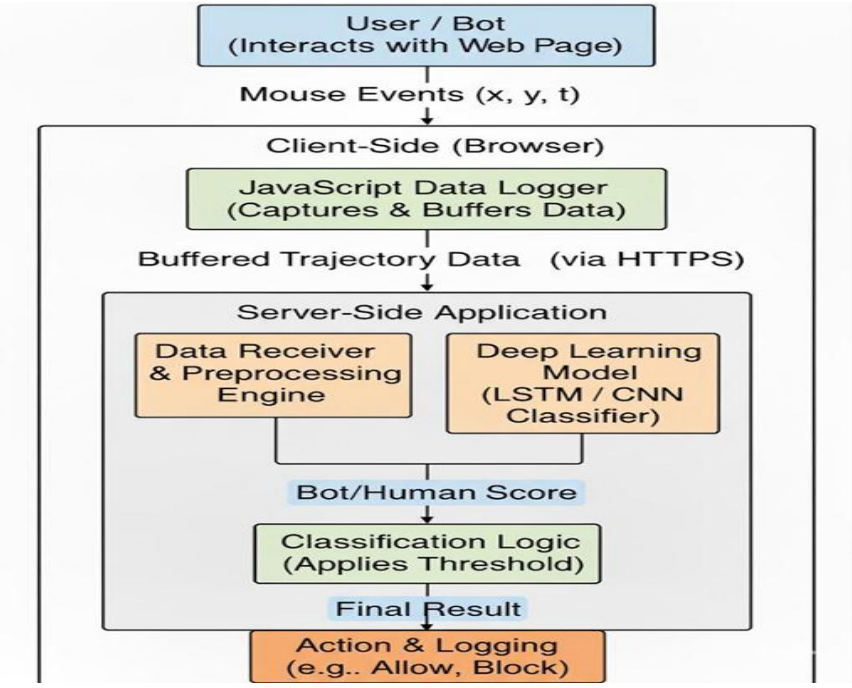

Fig. 1. *Architecture of the Mouse Dynamics Based Bot Detection System*

The system follows a client-server architecture. User interacts with a web-based login interface. Mouse movement data is captured in real-time. JavaScript collects events like move, click, and scroll. Data is sent to the backend server. Flask processes incoming data. Feature extraction is performed. Machine learning model predicts behavior. Results are returned to the frontend. A dashboard displays detection results. System ensures real-time performance. It is scalable and efficient.

Implementation Details

The system is developed using Flask for backend. Frontend is built using HTML, CSS, and JavaScript. Mouse events are captured dynamically. Data is stored in CSV format. Feature extraction includes velocity and acceleration. Angular movement is also analyzed. Statistical features are computed. Random Forest model is used for classification. Model is trained on human and bot data. External bot scripts simulate attacks. Real-time API handles prediction requests. Dashboard displays classification results. System handles errors effectively. NaN values are managed properly. Data cleaning improves accuracy. System supports continuous tracking. Testing is performed on multiple scenarios. Performance is optimized. Security is enhanced through behavior analysis.

Results and Discussion

The system successfully distinguishes humans and bots. Human interactions show irregular patterns. Bots show linear and predictable behavior. Detection accuracy is satisfactory. Real-time performance is achieved. Confidence scores provide reliability. Dashboard improves visualization. System works well in controlled demos. External bot detection is effective. Some edge cases exist for advanced bots. Short interactions may affect accuracy. Data quality impacts results. System performs efficiently overall. Future improvements can enhance accuracy.

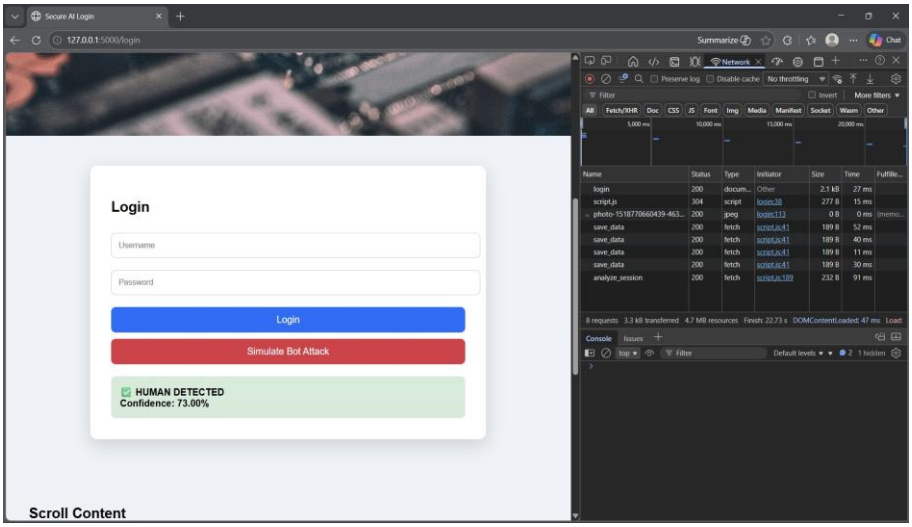

Fig. 2. *Login Interface*

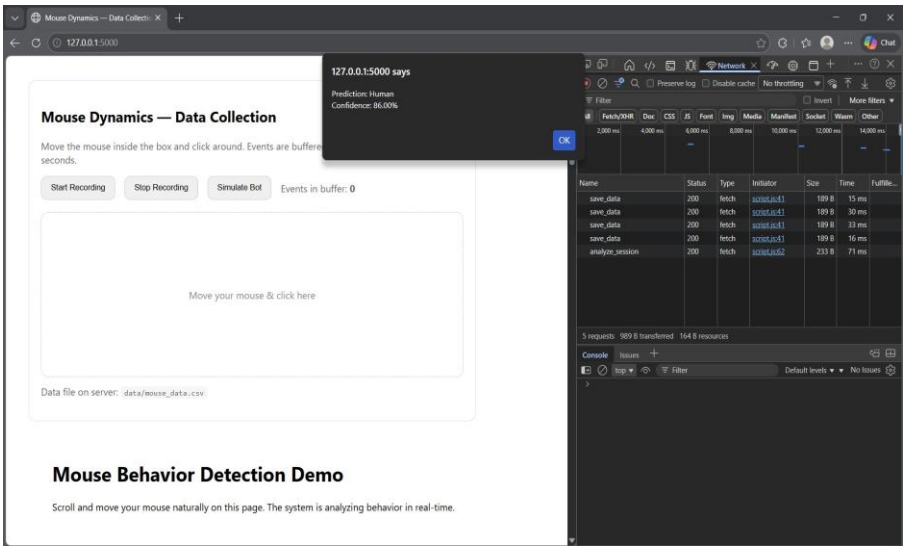

Fig. 3. *Data Collection Interface*

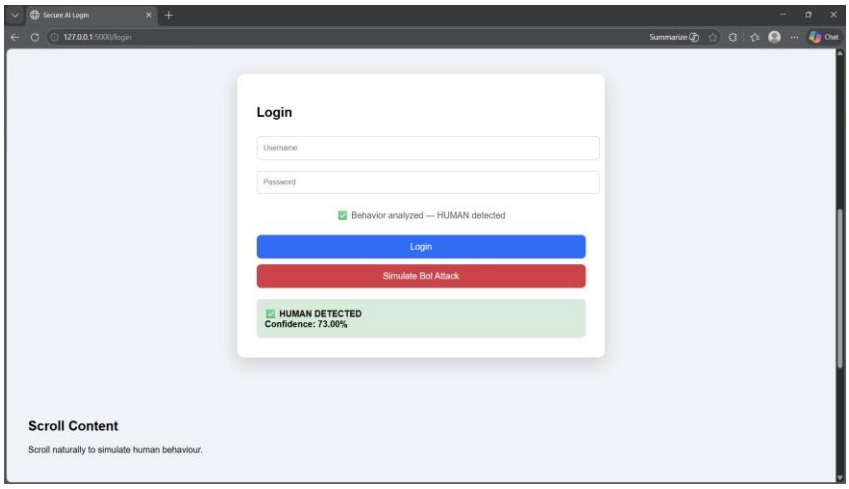

Fig. 4. *Human Detection Result*

Future improvements include better datasets. Advanced models can improve detection. Deep learning can be explored. System can detect more complex bots. Overall, system is effective and scalable.

References

1. A. Survey of Botnet and Botnet Detection Methods. *International Journal of Engineering Research and Technology*, 2013.
2. CyberPeace Foundation. "Who Is Winning the War with AI: Bots vs. CAPTCHA," 2024. Available: https://www.cyberpeace.org/resources/blogs/who-is-winning-the-war-with-ai-bots-vs-captcha
3. S. Hashia et al. "Mouse Dynamics Behavioral Biometrics: A Survey." *ResearchGate*, 2022.
4. F. Fourati et al. "Nonintrusive Behavioural Biometrics for Computer System Security," 2020.
5. S. Sadeghpour and N. Vlajic. "ReMouse Dataset: On the Efficacy of Measuring the Similarity of Human-Generated Trajectories for the Detection of Session-Replay Bots." *Journal of Cybersecurity and Privacy*, vol. 3, no. 1, pp. 95–117, 2023.
6. Radware. "4 Botnet Detection Techniques." Available: https://www.radware.com/cyberpedia/hot-management/4-botnet-detection-techniques
7. "A Survey on Botnet Detection Techniques." *ResearchGate*, 2020.
8. H. Niu, J. Chen, Z. Zhang, and Z. Cai. "Mouse Dynamics Based Bot Detection Using Sequence Learning." In *Biometric Recognition (CCBR 2021)*, Shanghai, China, pp. 49–56, 2021.
9. "User Authentication Based on Mouse Dynamics." *ResearchGate*, 2019.
10. M. A. A. Al-Qaness et al. "Using Deep Learning for Trajectory Classification." In *International Conference on the Quality of Information and Communications Technology*, 2021.
11. G. Kramida et al. "Mouse Behavior Classification Using Deep Learning." In *IEEE International Conference on Image Processing*, 2016.
12. A. Wei, Y. Zhao, and Z. Cai. "A Deep Learning Approach to Web Bot Detection Using Mouse Behavioral Biometrics." In *Lecture Notes in Computer Science*, 2019.
13. L. Zhao et al. "A Hybrid CNN-LSTM Model for Trajectory Prediction." *Sensors*, 2022.
14. M. Antal. "SapiMouse: A New Dataset for Mouse Dynamics." *GitHub Repository*, 2020. Available: https://github.com/margitantal68/sapimouse
15. S. Sadeghpour and N. Vlajic. "ReMouse Dataset: On the Efficacy of Measuring the Similarity of Human-Generated Trajectories for the Detection of Session-Replay Bots." *DBLP*, 2023.
16. S. Sadeghpour and N. Vlajic. "RanABD: MTD-Based Technique for Detection of Advanced Session-Replay Web Bots," 2023.
17. Center for Long-Term Cybersecurity (CLTC), University of California, Berkeley. "Adversarial Machine Learning." Available: https://cltc.berkeley.edu/anil/
18. Y. X. M. Tan et al. "Adversarial Attacks on Remote User Authentication Using Behavioural Mouse Dynamics." *arXiv Preprint*, arXiv:1905.11831, 2019.
19. Wikipedia. "Adversarial Machine Learning." Available: https://en.wikipedia.org/wiki/Adversarial_machine_learning
20. P. Singh. "Mouse Movement Behavioral Patterns Can Reliably Tell Bots from Humans," 2025.
21. I. Pozzana and E. Ferrara. "Measuring Bot and Human Behavioral Dynamics." *Frontiers in Physics*, 2020.
22. "Redefining Security: Unveiling the Vulnerabilities of CAPTCHA Mechanisms Using Deep Learning," ResearchGate, 2024.