User Identification based on Cursor Movements

Samriddh Singh samriddh20466@iiitd.ac.in
Varun Parashar varun20482@iiitd.ac.in
Shivam Kurda shivam21419@iiitd.ac.in
Dev Mann dev21382@iiitd.ac.in

***Abstract*—In our proposal, a supervised learning model that uses distinctive cursor motions to identify users is unveiled. We aim to create a sophisticated prediction system by utilizing labeled data that links cursor activities to specific individuals.**

I. Introduction

Based on a study conducted by Antal et al. [1], each user has a unique cursor movement when they navigate any application. This uniqueness can be observed in the trajectories exhibited by their mouse cursors, which are measured by recording the x and y coordinates along with timestamps. A set of 30 characteristics was determined in the study, including cursor speed, acceleration along the x and y axes, momentum, etc.

II. Related Work

"My Mouse, My Rules: Privacy Issues of Behavioral User Profiling via Mouse Tracking" by Luis A. Leiva, Ioannis Arapakis, and Costas Iordanou focuses on privacy issues brought about by user profiling through mouse tracking. Another work, **"Intrusion Detection using Mouse Dynamics (arXiv:1810.04668)"**, utilizes mouse movement patterns for intrusion detection, enhancing cybersecurity by analyzing behaviors and detecting anomalies.

III. Motivation

The popularity of online businesses has led to an increase in cybercrime, exploiting weak password-based protection. A revolutionary machine-learning method authenticates individuals by generating biometric profiles from movement patterns. This integrated approach strengthens security without interfering with user behaviors, countering the growing cyber threats.

IV. Applications

Cursor-based authentication offers versatile advantages across sectors, enhancing security in online banking, e-commerce, and remote work domains. It safeguards patient privacy in healthcare, augments data protection in government and education sectors, and fortifies remote data access in data centers. This strategy extends even to sensitive information scenarios.

V. Timeline

Week 1: Review recent research articles. Identify critical project research questions.
Week 2-3: Gather, clean, and format the data. Conduct data analysis to gain insights.
Week 4-5: Identify pertinent features in the data. Study relevant machine learning algorithms.
Week 6: Evaluate the performance of various machine learning algorithms.
Week 7: Select the optimal machine learning algorithm. Tune hyperparameters for best performance.
Week 8-9: Construct confusion matrices for different models. Plotting graphs showing error trends. Generate diagrams.
Week 10: Write up the project results.

VI. Individual Contributions

1. Research Paper Review: Everyone
2. Data Collection and Analysis: Samriddh and Varun
3. ML Model Exploration and Training: Everyone
4. Observations and Graphical Representation: Shivam and Dev
5. Documentation and Presentation: Everyone

References

[1] M. Antal and E. Egyed-Zsigmond, "Intrusion detection using mouse dynamics," *Journal of Computer Virology and Hacking Techniques*, vol. 16, no. 2, pp. 133–144, 2020.