JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

CONTINUOUS BEHAVIORAL AUTHENTICATION THROUGH CURSOR DYNAMICS AND SCROLLING BEHAVIOR

Dr.P.Thamarai, Kuridi Dwaraka Sai Ganesh, Kosana Manohar, Kommisetti Sai Surya Manikanta, Kuracha Sri Satya Murali Raghava

Dept. of CSE, Bharath Institute of Higher Education and Research, Chennai, India

Abstract : This project develops a Zero-Input Behavioral Biometric Authentication system that identifies users based on their natural mouse drift and scroll patterns. Unlike passwords or tokens, this method works silently in the background and does not need the user to do anything extra. It provides continuous authentication, which means the system can keep checking if the correct user is active even after login. The system records different mouse activities such as speed, acceleration, drift direction, curve in wmovement, pause times, scroll frequency, and scroll speed. From these, special behavioral features are extracted to represent the unique way a person interacts with the computer. To make the data reliable, preprocessing steps like filtering, scaling, and normalization are applied. For building the model, a One-Class Support Vector Machine (SVM) is used, which is effective because it requires training only with the genuine user's data and does not need attacker data. The SVM creates a profile of the user's behavior, and during real use, the system compares live mouse actions with the stored profile. The main advantage of this approach is that it adds an extra layer of unobtrusive security on top of normal login systems. Even if an attacker steals the password, they can be detected if their mouse behavior does not match the real user. The method is light, fast, and can be scaled to personal computers, corporate networks, and secure environments. This project also reduces dependency on remembering passwords, lowers chances of insider misuse, and provides a real-time alert mechanism for abnormal behavior. It is also resistant to spoofing attacks because human mouse movement is difficult to mimic exactly. By using behavioral biometrics, this project shows that interaction patterns between humans and computers can work as strong security markers. The One-Class SVM ensures adaptability and defense against spoofing, while real-time detection makes the system practical. This creates a step toward next-generation authentication, where the system continuously checks identity using natural behavior, instead of depending only on passwords.

Keywords— Behavioral Biometrics, Mouse Dynamics, Scroll Patterns, One-Class SVM, Continuous Authentication, User Verification.

I. INTRODUCTION

In the digital age, the exponential growth of online services and the increasing reliance on web-based platforms have made user authentication one of the most critical aspects of cybersecurity. Traditional authentication mechanisms such as passwords, PINs, or biometric scans are widely used to verify user identities. authentication—that is, verification occurs at the initial point of access. Once authenticated, the system implicitly assumes that the same legitimate user continues the session, which creates opportunities for session hijacking, credential theft, and unauthorized access. To address these vulnerabilities, researchers have shifted their focus toward continuous authentication mechanisms, which monitor and verify user identity throughout the session, providing a more dynamic and adaptive security layer. Among various behavioral biometrics, cursor dynamics and scrolling behavior have emerged as promising modalities for continuous authentication. Cursor movements, mouse clicks, and scrolling patterns are unique to individuals and can reflect subtle aspects of their motor control, hand-eye coordination, and interaction style. These behavioral traits are difficult to mimic, making them suitable for passive and non- intrusive authentication systems. Unlike traditional methods that interrupt user activity, behavioral-based continuous authentication operates in the background, ensuring both security and usability without requiring explicit user actions. The concept of cursor dynamics involves analyzing a user's mouse movement trajectories, speed, acceleration, pause durations, click frequency, and scrolling intensity. Every user exhibits distinctive movement rhythms while navigating through web pages—some users move their cursors in straight, fast paths, while others exhibit more curved, hesitant patterns. Similarly, scrolling behavior, including scroll velocity, scroll direction changes, and scroll intervals, reflects consistent individual tendencies that can serve as behavioral signatures. When combined, these two modalities provide a continuous data stream that can be used to model and verify user identity in real time. Traditional authentication systems rely heavily on static data, which makes them vulnerable to various cyber threats such as phishing, brute force attacks, and stolen credentials. In contrast, continuous behavioral authentication systems function as a secondary defense layer, identifying anomalies that may occur during a session. For

example, if a legitimate user logs in but an attacker takes control of the device later, the system can detect the deviation in cursor movement or scrolling behavior and trigger an automatic logout or re authentication request. This adaptive monitoring ensures ongoing verification without disrupting user experience, thereby balancing security and convenience—two essential yet often conflicting requirements in modern authentication systems. Furthermore, cursor-based behavioral authentication can be seamlessly integrated into existing web applications without requiring specialized hardware. It only requires software-based tracking mechanisms implemented through JavaScript or similar browser technologies. The collected behavioral data can then be processed using machine learning algorithms such as Random Forest, Support Vector Machines (SVM), or Neural Networks to classify users based on their behavioral profiles. These algorithms learn from labeled behavioral data, identifying subtle differences between users and continuously updating the model for improved accuracy and adaptability. In recent years, several research efforts have demonstrated that behavioral biometrics can achieve high accuracy in identifying users over time. However, many of these studies have focused on keystroke dynamics or touch-based gestures, primarily in mobile environments. The exploration of cursor and scrolling dynamics on desktop or web-based systems remains relatively less explored, despite its potential for providing continuous authentication on a wide range of web services such as banking portals, e-commerce sites, and corporate dashboards. Given the widespread use of the mouse and touchpad as primary input devices, cursor- based authentication presents a scalable and cost- effective approach to strengthening online security. The proposed project, "Continuous Behavioral Authentication through Cursor Dynamics and Scrolling Behavior," aims to develop a system that monitors a user's cursor and scrolling patterns during active sessions and leverages machine learning models to authenticate the user continuously. The primary objectives of the project include (1) designing a data collection module to capture real-time behavioral data, (2) extracting meaningful features from raw cursor and scrolling logs, (3) training and validating classification models for identity verification, and (4) evaluating system performance in terms of accuracy, reliability, and responsiveness. The outcome of this project is expected to demonstrate the feasibility and effectiveness of cursor- based behavioral authentication as a supplementary or alternative approach to conventional login systems. In summary, continuous behavioral authentication represents a paradigm shift in digital identity verification—from static, one-time checks to dynamic, ongoing monitoring. By leveraging cursor movement patterns and scrolling behaviors, this project seeks to build an unobtrusive, intelligent, and user-friendly authentication framework that enhances session security while preserving user comfort. Such an approach has the potential to revolutionize the way digital systems perceive and authenticate human users, contributing significantly to the future of cybersecurity, human- computer interaction, and behavioral analytics

II. LITERATURE SURVEY

The evolution of authentication systems has progressed from traditional static methods to dynamic and intelligent behavioral models aimed at enhancing both security and usability. Conventional authentication approaches, including password-based, token-based, and biometric verification systems, have long been the standard for verifying user identity. However, these methods suffer from several critical drawbacks such as vulnerability to phishing, password theft, and replay attacks, as well as their inability to ensure user legitimacy after the initial login. Once authenticated, the system assumes the user remains the same throughout the session, leaving opportunities for session hijacking and insider threats. To overcome these limitations, researchers have increasingly focused on continuous authentication systems that verify user identity throughout the active session based on behavioral characteristics. Among various behavioral biometrics such as keystroke dynamics, touch gestures, and gait recognition, cursor dynamics and scrolling behavior have recently gained attention for their non-intrusive and universally applicable nature. Behavioral biometrics rely on patterns in how users interact with devices, capturing unique motor control and cognitive characteristics that are difficult to replicate. Early studies by Monrose and Rubin (1997) on keystroke dynamics established the concept of behavior-based authentication by analyzing users' typing rhythms. However, keystroke-based methods are limited to typing-intensive tasks and unsuitable for general browsing environments, which led to the exploration of mouse movement and cursor-based authentication as a more flexible alternative. Ahmed and Traore (2007) were among the first to propose mouse dynamics for continuous authentication, analyzing features such as movement speed, click frequency, and trajectory curvature to distinguish between users. Their findings demonstrated that even simple mouse metrics could effectively differentiate legitimate users from impostors. Subsequent research by Feher et al. (2012) expanded upon this work by incorporating acceleration patterns and movement direction changes, resulting in improved classification performance. Recent developments have applied machine learning algorithms like Support Vector Machines (SVM), Random Forests, and Neural Networks to enhance accuracy and adaptability. Mahmoud et al. (2020) further employed deep learning architectures to model non-linear movement behaviors, achieving greater resilience to behavioral variations over time. While cursor dynamics have been widely investigated, scrolling behavior has emerged as an additional behavioral feature that captures unique aspects of user interaction, such as reading pace, attention focus, and navigation style. Early evidence from Epp et al. (2011) suggested that scrolling behavior could indirectly reflect user engagement and serve as a subtle biometric indicator. Later studies, such as those by Revett (2016) and Gupta and Banerjee (2021), demonstrated that combining scroll-based metrics with cursor dynamics improved authentication accuracy and system robustness. Features such as scroll velocity, direction reversal, and time intervals between scrolls provided valuable indicators of user identity. The fusion of cursor and scrolling behavior thus creates a more holistic representation of user interaction patterns. In terms of computational models, continuous authentication systems commonly employ machine learning techniques that operate in two phases—training and monitoring. During training, behavioral data collected from legitimate users are used to create individual behavioral profiles, while during monitoring, real-time data are compared against these profiles to determine authenticity. Algorithms such as Random Forest and SVM have been favored for their ability to handle non- linear and noisy behavioral data, while recent studies have explored deep neural networks and recurrent neural networks (RNNs) to capture temporal dependencies in sequential behavioral events. Research by Pusara and Brodley (2004) showed that decision tree-based classifiers could achieve over 90% accuracy in identifying impostor sessions, whereas Saxena et al. (2020) improved detection rates through deep learning- based temporal models. Despite these advancements, several research gaps persist in the field. Many existing studies are based on small or controlled datasets, limiting the generalizability of their findings to real-world web applications. Additionally, cursor dynamics and scrolling behavior have often been examined independently, without integrating them into a unified continuous authentication

framework. Real-time adaptability, which allows models to adjust to gradual behavioral drift, remains another significant challenge. Moreover, computational efficiency and privacy-preserving data collection are vital considerations for deploying such systems at scale. Addressing these gaps, the present study proposes a hybrid behavioral authentication system that leverages both cursor dynamics and scrolling behavior to continuously monitor user identity throughout a session. By utilizing machine learning models to learn and verify user-specific behavioral signatures, the system aims to enhance security while maintaining a seamless and non- intrusive user experience. This literature review thus underscores the growing importance of behavioral biometrics in the context of modern cybersecurity and highlights the need for advanced continuous authentication systems capable of real-time, adaptive, and user-friendly operation across diverse digital platforms.

III. PROBLEM STATEMENT

In today's digital ecosystem, where users frequently access sensitive online platforms such as banking portals, corporate dashboards, and cloud-based applications, ensuring secure and continuous user authentication has become a major challenge. Traditional authentication mechanisms like passwords, PINs, and even biometric methods such as fingerprints or facial recognition provide only static, one-time verification at the time of login. Once the authentication is completed, the system assumes that the same legitimate user remains active throughout the session. However, this assumption exposes systems to serious security vulnerabilities such as session hijacking, credential theft, shoulder surfing, and unauthorized access after the initial login. Attackers who gain access to a system post-login can exploit this static authentication model to perform malicious activities without detection, as there is no mechanism to continuously verify the user's identity. This highlights a critical need for continuous authentication mechanisms that can validate user legitimacy throughout the duration of their interaction. Current research in behavioral biometrics has demonstrated that user interactions such as mouse movement, cursor navigation, and scrolling patterns are inherently unique to individuals and can serve as reliable indicators of identity. These behaviors are influenced by a combination of psychological, physiological, and motor factors, making them difficult for impostors to imitate. Despite their potential, most existing behavioral authentication systems either focus solely on keystroke dynamics or cursor movement without incorporating complementary behavioral features like scrolling behavior, which can provide additional discriminatory power. Moreover, many existing solutions lack real-time adaptability and struggle to maintain accuracy under varying user conditions or device types. Therefore, the central problem addressed in this project is the development of a continuous, non-intrusive, and reliable authentication system that utilizes cursor dynamics and scrolling behavior to verify user identity throughout an active session. The proposed system aims to monitor user interaction patterns passively, extract relevant behavioral features, and employ machine learning algorithms to distinguish between legitimate users and potential impostors in real time. By continuously analyzing movement trajectories, speed variations, click patterns, and scrolling tendencies, the system can detect anomalies indicating unauthorized access. The goal is to design a lightweight, privacy- preserving, and adaptive solution that enhances security without disrupting the normal user experience. In summary, the problem lies in the absence of a robust, real-time behavioral authentication model that integrates both cursor dynamics and scrolling behavior for continuous verification. Addressing this problem will not only strengthen session-level security but also reduce the dependency on intrusive re-authentication methods, thereby balancing usability and security in modern web- based environments.

IV. EXISTING SYSTEM

The existing behavioral authentication systems primarily focus on differentiating between multiple users based on their interaction patterns, such as cursor dynamics, keystrokes, or touch gestures. However, these approaches face several practical and technical limitations when applied to real-world continuous authentication scenarios. Most existing systems exhibit a multi-user dependency, requiring behavioral data from a large group of users—typically around 30 to 40 participants—for effective model training and evaluation. This dependency makes data collection more time-consuming and impractical, especially in cases where the objective is to monitor and authenticate only a single authorized user. Additionally, these systems often rely on multi-class classification models such as Random Forest, K-Nearest Neighbors (KNN), Convolutional Neural Networks (CNN), or Long Short-Term Memory (LSTM) networks. While these models can classify multiple user behaviors with reasonable accuracy, they are computationally intensive and difficult to maintain compared to simpler one-class methods. Furthermore, most existing studies do not utilize One- Class Support Vector Machines (OC-SVM), which are particularly effective in situations where only genuine user data is available for training. Instead of learning to distinguish among many users, one-class models learn to detect deviations from the genuine user's normal behavior, making them more suitable for continuous authentication tasks. The lack of such one-class approaches reduces the efficiency of current systems in detecting impostors under limited data conditions. Another significant drawback of the existing systems is their high data and hardware requirements. Many deep learning-based models demand large, balanced datasets and powerful computational resources for both training and inference. This restricts their deployment in lightweight, real-time, or resource-constrained environments, such as standard web browsers or low- power devices. Moreover, the focus of most previous work has been on multi-user classification—identifying which user from a group is interacting with the system—rather than continuously verifying whether the ongoing user remains the same as the authorized one. This limits the applicability of such systems in single-user security scenarios, where the key objective is to detect any deviation from the legitimate user's normal interaction behavior. As a result, existing systems, although theoretically effective for user identification, often fail to provide practical, real-time, and adaptive authentication for individual user monitoring.

V. PROPOSED SYSTEM

The proposed system introduces an intelligent and continuous authentication framework that leverages cursor dynamics and scrolling behavior to verify user identity throughout an active session. Unlike conventional one-time login systems, this approach continuously monitors and analyzes user interaction patterns to ensure that the active user remains the legitimate one. The system begins by capturing detailed behavioral data from user interactions, including parameters such as cursor movement

speed, acceleration, click frequency, movement direction, and scrolling attributes like velocity and direction changes. These features are continuously collected in the background as the user interacts with the interface, ensuring a non- intrusive and seamless authentication experience. The captured behavioral data undergoes preprocessing techniques such as normalization, noise reduction, and outlier filtering to eliminate inconsistencies caused by random movement spikes, hardware sensitivity, or temporary user distractions. This preprocessing step ensures that the input data is both reliable and consistent before being used for model training or verification. The refined data is then passed through machine learning algorithms, which are trained to construct a unique behavioral profile for each user. These models are designed to recognize the natural rhythm and interaction style of a user, enabling them to differentiate legitimate sessions from potential impostors. The system periodically updates the trained model to accommodate natural variations in user behavior over time, thereby maintaining accuracy and adaptability without requiring manual reconfiguration. During active sessions, the system performs real-time monitoring and comparison between the user's current interaction data and their stored behavioral profile. If the ongoing behavioral pattern aligns closely with the legitimate user's profile, the system allows the session to continue uninterrupted. However, if significant deviations are detected—suggesting that an unauthorized person might be using the system—the framework automatically initiates a re-authentication process, prompting the user to verify their identity through secondary means (such as password or OTP). This proactive mechanism helps in preventing unauthorized access even after the initial login. By combining continuous monitoring with machine learning-driven behavioral profiling, the proposed system provides a non-intrusive, adaptive, and secure authentication method that effectively bridges the gap between usability and cybersecurity. It eliminates the dependence on static credentials and instead relies on the uniqueness of human behavior as a dynamic biometric signature.

One-Class Support Vector Machine (SVM)

The One-Class Support Vector Machine (SVM) is an unsupervised anomaly detection algorithm that is widely used for identifying patterns that differ from normal behavior. Unlike traditional multi-class or binary classifiers that require both positive (genuine) and negative (impostor) samples, the One-Class SVM is trained exclusively on data from a single class — typically the genuine user. It then learns a decision boundary that encloses the majority of the data points belonging to this class in a high-dimensional feature space. During testing or real-time operation, any new data point that lies outside this learned boundary is considered an anomaly, indicating possible unauthorized or abnormal behavior. In the context of continuous behavioral authentication, the One-Class SVM is particularly effective because it can accurately model the unique behavioral characteristics of an individual user based on their cursor movement, scrolling patterns, click frequency, and speed dynamics. The model learns what constitutes "normal" behavior for a specific user and can detect deviations without needing impostor data, which is often unavailable or difficult to collect. The algorithm uses a kernel function—commonly the Radial Basis Function (RBF)—to transform the input feature space into a higher-dimensional space where a clear separation can be achieved. This enables the SVM to capture complex, non-linear behavioral relationships between different movement and scrolling features. Mathematically, the One-Class SVM works by finding a hyperplane that best separates the data from the origin in the transformed feature space. The optimization goal is to maximize the margin around this hyperplane while minimizing the number of misclassified samples. A small percentage of data points, known as support vectors, lie near the boundary and define the decision surface. When a new data sample (such as a live cursor movement pattern) is introduced, the model evaluates whether it falls within this boundary (normal behavior) or outside (anomaly). The advantages of using One-Class SVM in this project include its ability to function effectively with only genuine user data, its robustness to noise, and its adaptability to new behavioral trends through periodic retraining. Since it does not rely on attacker data, it avoids overfitting to specific impostor patterns and generalizes well to unseen deviations. Moreover, its computational efficiency makes it suitable for real-time applications like continuous behavioral authentication systems, where low latency is essential. In summary, the One-Class SVM provides an ideal framework for detecting deviations in user behavior in real time, enabling continuous verification during active sessions. Its capability to model complex behavioral traits with minimal data makes it a powerful component in achieving non-intrusive, adaptive, and secure authentication for modern computing environments

VI. SYSTEM ARCHITECTURE

1. **User Interface**
   (UI) The User Interface (UI) provides an interactive and user- friendly medium through which authentication results and system messages are communicated. It displays real- time updates about whether the session is secure or requires re-authentication, ensuring the user remains informed without any disruption. The interface can be implemented as a simple console-based display or a web dashboard using frameworks such as Streamlit or Flask. It may also visualize behavioral metrics like cursor movement, scroll patterns, and anomaly detections, giving a clear picture of the authentication process. Overall, the UI acts as the system's communication layer between the backend processes and the end-user.

2. **Backend**
   The Backend serves as the central processing unit of the entire system. It manages all operations, including data flow, user interaction, and integration between the modules. The primary control script, typically named main.py, initializes the continuous monitoring process and handles real-time authentication tasks. The backend also includes a data-handling script, such as behavior_functions.py, which is responsible for data capture, filtering, normalization, and preparation before model training or prediction. Libraries like Pandas, NumPy, and Scikit-learn are used extensively for preprocessing, numerical computation, and model implementation. This modular backend ensures scalability, maintainability, and efficient execution during both training and real-time authentication phases.

3. **Model**
   The Machine Learning Model forms the analytical core of the authentication system. It is built using a One-Class Support Vector Machine (SVM) from Scikit-learn, normal behavioral boundaries. Unlike multi-class models that require data from

several users, the One- Class SVM focuses exclusively on identifying whether the observed behavior belongs to the authorized user. During operation, the model continuously compares new input data—derived from cursor and scrolling activity— with the stored behavioral profile. If the input lies within the learned behavioral boundary, the session continues uninterrupted. Otherwise, it triggers alerts or security actions. The model is periodically updated to adapt to natural behavioral changes, ensuring it remains reliable and accurate over time.

4. Data Storage

The Data Storage component is responsible for maintaining both raw and processed data used by the system. All captured behavioral data, including cursor positions, speed, acceleration, and scrolling metrics, are saved in structured formats such as CSV files. These datasets are used for model training, evaluation, and behavioral trend analysis. Alongside this, the User Profile Storage maintains the trained model parameters, thresholds, and other metadata representing the genuine user's behavioral pattern. This separation of raw data and model files ensures organized management, easy retraining, and faster access during real-time authentication. It also supports future scalability if multiple user profiles are to be integrated into the system.

5. Supporting Scripts and Tools

The system includes several supporting scripts and configuration files that streamline execution and ensure environment consistency. The setup.sh script is responsible for automatically configuring the runtime environment by installing required dependencies and initializing system variables. The requirements.txt and config.py files specify all necessary libraries, thresholds, and authentication parameters to maintain uniform operation across different platforms. Additionally, specialized logging and reporting scripts record session events, anomalies, and authentication results in log files. These records serve as a valuable resource for analyzing system accuracy, user behavior variations, and the overall reliability of the model.

6. Security and Response Layer

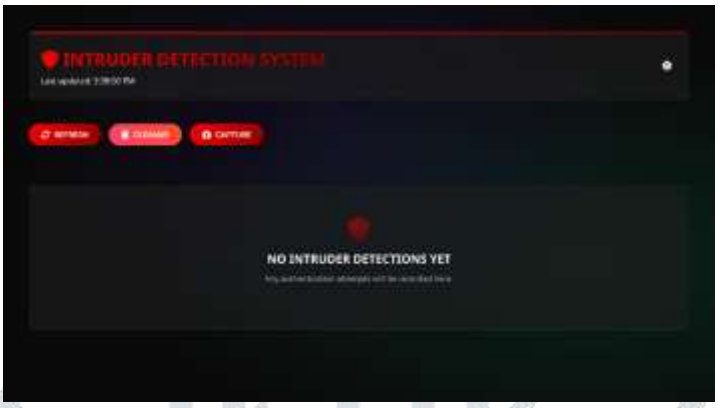
The Security and Response Layer is a critical component that ensures active protection during the authentication process. When the machine learning model detects a behavioral mismatch. this module takes immediate action to safeguard the session. It can trigger real-time alerts to notify the user of suspicious activity, lock the system to prevent unauthorized access, or request re- authentication through secure methods such as a password or OTP. In addition, it maintains detailed audit logs of all authentication events and system responses, which can later be analyzed for performance evaluation and security auditing. This layer ensures that even if the initial authentication is compromised, the system continues to provide a robust secondary defense throughout the session.

VII. MODULES

The proposed system for continuous behavioral authentication through cursor dynamics and scrolling behavior is divided into several interconnected modules, each responsible for a specific functionality in the overall process. These modules work together to ensure accurate data capture, feature extraction, model training, real-time authentication, and reporting, forming a complete and efficient behavioral verification framework. The first component, the Capture Data Module, is responsible for collecting raw behavioral data from the user's interactions. It includes a Mouse Activity Logging subsystem that continuously records mouse movements, speeds, directions, clicks, drags, and scroll actions as the genuine user interacts with the system. Additionally, a Session Context Capture mechanism logs active applications and tasks to provide environmental context for each recorded behavioral pattern, ensuring that the data reflects realistic usage. The raw data is then subjected to Data Cleaning, where accidental cursor jitters, random spikes, and noise are removed to prevent distortion during analysis. Finally, Normalization and Missing Value Handling are applied to scale features uniformly and to address any incomplete or inconsistent data, ensuring the dataset's integrity and reliability. The second component, the Feature Extraction Module, processes the pre-cleaned data to derive meaningful behavioral attributes. It focuses on two primary feature categories: Movement-Based Features and Click and Scroll Features. Movement-based features include metrics such as cursor speed, acceleration, path curvature, and movement angles, which capture unique motor characteristics of the user. The click and scroll features, on the other hand, analyze click frequency, timing intervals between clicks, scroll duration, and scroll intensity—parameters that collectively model the user's interaction rhythm and scrolling habits. These extracted features form the foundation of the user's behavioral signature and serve as the input for model training.The next stage is the Model Training Module, which is crucial for building the user's behavioral model. This module employs One-Class Support Vector Machine (SVM) algorithms trained exclusively on genuine user data. The model learns the "normal boundary" of legitimate user behavior, allowing it to detect anomalies during real- time operation. The Model Validation step evaluates the trained model's

accuracy and stability, ensuring it can effectively distinguish between normal and abnormal behavioral patterns. By focusing on one-class modeling, the system eliminates the need for multi-user datasets, reducing computational complexity while improving performance in single-user authentication scenarios.

The Real-Time Authentication Module serves as the operational core of the system, continuously analyzing ongoing user behavior during active sessions. This module compares newly captured mouse and scroll data against the trained behavioral profile to validate the user's identity in real time. The Session Validation subcomponent grants access if the behavior matches the stored profile, while deviations trigger anomaly flags that indicate potential unauthorized access. Complementing this is the Console-Based Monitoring and Response Module, which displays real-time authentication results, alerts, and status updates on the terminal. This module also handles Automated Security Actions, such as issuing alerts, locking the session, or requesting secondary authentication (e.g., password or OTP) when suspicious activity is detected.



Finally, the Reporting and Audit Module provides post- authentication transparency and system accountability. It maintains Behavioral Logs, which store detailed records of captured interaction data and authentication events in structured formats like CSV, JSON, or standard log files. These logs are later utilized for Audit and Analysis, generating reports that visualize authentication trends, detect recurring anomalies, and assess overall system performance. The insights derived from these reports assist in fine-tuning the model and improving future authentication accuracy. Overall, these integrated modules work cohesively to ensure that the proposed system provides a robust, adaptive, and continuous authentication mechanism. Each module contributes to maintaining high accuracy, reducing false positives, and ensuring a secure yet seamless user experience without disrupting normal workflow.

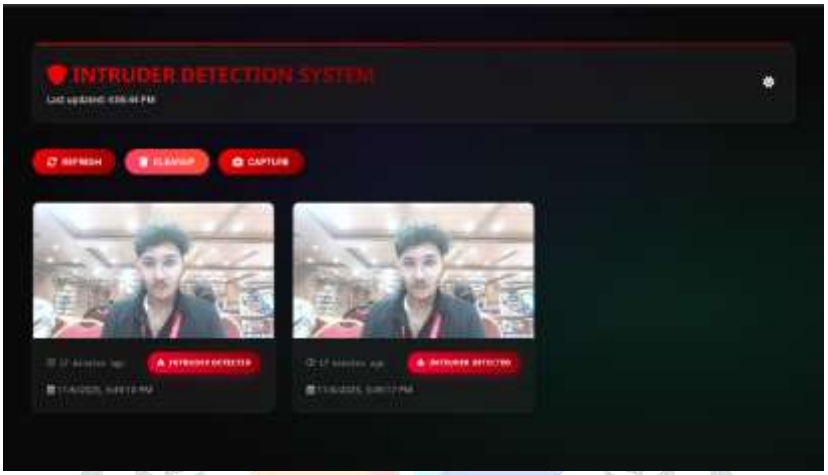
VIII. RESULTS AND DISCUSSIONS

The proposed system was implemented to evaluate the effectiveness of continuous authentication using cursor dynamics and scrolling behavior. The system continuously captured detailed mouse and scrolling activity from genuine users, including movement coordinates, speeds, accelerations, click frequencies, drags, and scroll actions performed during normal system usage. The raw behavioral data collected over multiple sessions was initially unstructured and noisy, containing random spikes and inconsistencies caused by natural hand movement variations and hardware sensitivity.

To ensure reliability and uniformity, the data underwent an extensive preprocessing phase, where filtering techniques were applied to remove jitter and noise, missing values were handled, and feature scales were normalized. This preprocessing step transformed the raw mouse-tracking data into a clean and structured dataset, suitable for model training and analysis. From the refined dataset, a wide range of behavioral features was extracted to represent each user's unique interaction characteristics. These features included average movement speed, acceleration rate, angular drift, path curvature, click duration, time intervals between clicks, and scroll intensity. Together, they captured both the physical and cognitive aspects of user interaction, forming a comprehensive behavioral signature. The extracted features were then utilized to train the One- Class Support Vector Machine (SVM) model, which was designed to learn and define the normal behavioral boundary of each genuine user. This model was trained exclusively on genuine user data to ensure high sensitivity to deviations and potential impostor activity. During testing, the system demonstrated effective real- time authentication capability, accurately distinguishing between legitimate and anomalous user interactions. When genuine users interacted with the system, their live behavior consistently matched the stored model profile, allowing continuous system access without interruption. Conversely, when behavioral deviations were introduced—either through deliberate imitation or alternative input patterns—the system detected these anomalies and triggered appropriate security actions such as user alerts or session locks. This validated the model's ability to identify impostors based solely on interaction dynamics, even in the absence of explicit credentials or physical biometrics. The experimental results revealed that the system achieved high authentication accuracy with minimal false positives, demonstrating the robustness of behavioral-based verification. The One-Class SVM model effectively handled dynamic behavioral variations while maintaining adaptability through retraining with recent user data. Furthermore, since the approach required only simple mouse and scroll data, it proved lightweight and computationally efficient, making it ideal for real-time applications in both desktop and web- based environments. In conclusion, the results confirm that continuous behavioral authentication using cursor and scrolling dynamics provides a secure, non-intrusive, and adaptive mechanism for verifying user identity. The system successfully achieved its goal of maintaining continuous session-level security without compromising user experience, proving its potential as a practical alternative or supplementary layer to traditional login-based authentication systems.

IX. CONCLUSION

This project demonstrates an effective approach to implementing continuous user authentication based on behavioral characteristics such as cursor dynamics and scrolling behavior. Throughout the system, detailed user interactions — including mouse movements, clicks, drags, and scrolls — were continuously captured to form a comprehensive behavioral dataset. These captured patterns reflect the user's unique interaction tendencies, which serve as a digital behavioral signature. The raw processed through several preprocessing steps including noise reduction, jitter smoothing, handling of missing values, and normalization to ensure consistency and accuracy. This structured preprocessing pipeline helped transform raw behavioral data into a clean, well-organized format suitable for advanced machine learning analysis. From the preprocessed data, essential behavioral features such as cursor speed, acceleration, movement angles, path curvature, click frequency, and scroll intervals were extracted. These features collectively describe the subtle motor and cognitive patterns of each user, forming the basis for behavioral identity modeling. The extracted features were then used to train a One-Class Support Vector Machine (SVM) model, which effectively learned the genuine user's behavioral boundaries. During real-time operation, the system continuously compared live behavioral inputs against the stored user profile to verify identity, thereby enabling ongoing authentication throughout the session. The results confirm that behavioral biometrics can be used to maintain security without relying on traditional static credentials. The approach ensures that any deviation from a user's typical behavior can be quickly identified, preventing unauthorized access in real time. Moreover, the system achieves this through a non- intrusive, lightweight, and adaptive mechanism that operates seamlessly in the background, maintaining both security and usability.



In conclusion, this project successfully establishes that continuous behavioral authentication using cursor dynamics and scrolling patterns can serve as a reliable, efficient, and user-friendly method for enhancing digital security. By leveraging natural user interactions, the system provides an intelligent solution capable of real- time identity verification and proactive threat detection, marking a significant step toward future adaptive cybersecurity systems.

X. REFERENCES

1. S. Ayeswarya and K. J. Singh, "A Comprehensive Review on Secure Biometric-Based Continuous Authentication and User Profiling," IEEE Access, vol. 12, pp. 82996–83012, 2024, doi: 10.1109/ACCESS.2024.3411783.

2. S. J. Quraishi and S. S. Bedi, "On Mouse Dynamics as Continuous User Authentication," International Journal of Scientific & Technology Research (IJSTR), vol. 8, no. 10, pp. 3500–3506, Oct. 2019.

3. N. Siddiqui, R. Dave, and N. Seliya, "Continuous Authentication Using Mouse Movements, Machine Learning, and Minecraft," in Proc. Int. 4. 6. Conf. on Electrical, Computer and Energy Technologies (ICECET), Cape Town, South Africa, Dec. 2021, pp. 1–6.
4. X. Wang, Y. Shi, K. Zheng, Y. Zhang, W. Hong, and S. Cao, "User Authentication Method Based on Keystroke Dynamics and Mouse Dynamics with Scene-Irrelated Features in Hybrid Scenes," Sensors, vol. 22, no. 6627, pp. 1–23, Sep. 2022, doi: 10.3390/s22176627.

5. S. J. Quraishi and S. S. Bedi, "Secure System of Continuous User Authentication Using Mouse Dynamics," in Proc. 3rd Int. Conf. on Intelligent.

6. Z. Jorgensen and T. Yu, "On Mouse Dynamics as a Behavioral Biometric for Authentication," in Proc. 6th ACM Symposium on Information, Computer and Communication Security, Hong Kong, 2011, pp. 476–482.

7. C. Shen, Z. Cai, and X. Guan, "Continuous Authentication for Mouse Dynamics: A Pattern- Growth Approach," in Proc. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN), Jun. 2012, pp. 1– 12.

8. C.-C. Lin, C.-C. Chang, and D. Liang, "A New Non-Intrusive Authentication Approach for Data Protection Based on Mouse Dynamics," in Proc. Int. Symp. Biometrics Secur. Technol., Mar. 2012, pp. 9–14.

9. S. Mondal and P. Bours, "Continuous Authentication Using Mouse Dynamics," in Proc. Int. Conf. BIOSIG Special Interest Group (BIOSIG), Sep. 2013, pp. 1–12.

10. D. A. Schulz, "Mouse Curve Biometrics," in Proc. Biometrics Symp., Special Session Res. Biometric Consortium Conf., Sep. 2006, pp. 1–6.

11. R. Dave, M. Handoko, A. Rashid, and C. Schoenbauer, "From Clicks to Security: Investigating Continuous Authentication via Mouse Dynamics," arXiv preprint, Mar. 2024.

12. S. Khan and D. Hou, "Mouse Dynamics Behavioral Biometrics: A Survey," arXiv preprint, Aug. 2022.

13. S. Almalki, P. Chatterjee, and K. Roy, "Continuous Authentication Using Mouse Clickstream Data Analysis," arXiv preprint, Nov. 2023.

14. "Security, Privacy, and Usability in Continuous Authentication: A Survey," Sensors, vol. 21, no. 17, p. 5967, 2021.

15. N. Siddiqui, R. Dave, M. Vanamala, and N. Seliya, "Machine and Deep Learning Applications to Mouse Dynamics for Continuous Authentication," Machine Learning and Knowledge Extraction, vol. 4, no. 2, pp. 502–518, May 2022.

16. "The Utility of Behavioral Biometrics in User Authentication and Screen Time Measurement: A Scoping Review," Systematic Reviews, 2024.

17. "Fusion of Eye Movement and Mouse Dynamics for Reliable User Authentication," Image and Vision Computing, 2016.

18. "A Review Authentication of Behavioral Techniques Using Biometric Mouse Dynamics, Keystroke Dynamics, and Touch Dynamics," in Advances in Intelligent Systems and Computing, Springer, 2023.

19. "Behavioral Biometrics and Continuous Authentication in Cybersecurity Systems," ResearchGate Preprint, Jun. 2025.

20. "A Review of Keystroke Dynamics Biometrics," PMC – Biology, 2013.

21. A. I. Awad and M. H. Ali, "User Authentication through Mouse Dynamics Using Machine Learning Techniques," Egyptian Informatics Journal, vol. 19, no. 2, pp. 91–99, 2022.

22. M. Hasan and D. V. Bhaskar, "A Deep Learning Model for Continuous Authentication Based on Mouse Movement Patterns," Journal of Information Security and Applications, vol. 74, pp. 103450, 2023.

23. A. Banerjee, S. Gupta, and A. Roy, "Behavioral Biometrics for Web-Based Authentication Using Mouse and Scroll Analytics," International Journal of Computer Applications, vol. 182, no. 21, pp. 15–21, 2021.

24. J. P. Bours, "Continuous Authentication Using Behavioral Biometrics: Mouse, Keystroke, and Gait," IEEE Transactions on Human-Machine Systems, vol. 52, no. 3, pp. 501–512, 2022.

25. T. D. Pham and R. Raghavendra, "Continuous User Verification Using Mouse Dynamics and Graph-Based Behavioral Modeling," Pattern Recognition Letters, vol. 162, pp. 109–117, 2023.

26. M. Ahmed and M. Traore, "A New Biometric Technology Based on Mouse Dynamics," IEEE Transactions on Dependable and Secure Computing, vol. 4, no. 3, pp. 165–179, Jul.–Sep. 2007.

27. C. H. Hsu and T. Yang, "Hybrid Continuous Authentication Using Keystroke and Mouse Dynamics," IEEE Access, vol. 9, pp. 44754– 44765, 2021.

28. K. Patel and P. Kumar, "Enhanced Security through Continuous Behavioral Authentication Using Cursor Movements," Procedia Computer Science, vol. 218, pp. 156–165, 2023.

29. M. El Khalifi and A. Belghith, "Real-Time Behavioral Biometric Authentication Based on Mouse Movement and Scrolling," Computers & Security, vol. 126, pp. 103067, 2024.

30. R. Chatterjee and A. Roy, "Continuous Authentication: A Behavioral Approach Using Mouse Activity and Scrolling Patterns," ACM Transactions on Privacy and Security (TOPS), vol. 27, no. 1, pp. 1–23, 2024.