# AI-Powered Behavioral Biometrics for Continuous Authentication

1st Shobha K
*Department of Computer Science & Engineering*
*Siddaganga Institute of Technology*
Tumakuru, India
shobhak@sit.ac.in

2nd Ananya Kathal
*Department of Computer Science & Engineering*
*Siddaganga Institute of Technology*
Tumakuru, India
4si21cs063@sit.ac.in

2nd Archita Singh
*Department of Computer Science & Engineering*
*Siddaganga Institute of Technology*
Tumakuru, India
4si21cs072@sit.ac.in

2nd Krish U
*Department of Computer Science & Engineering*
*Siddaganga Institute of Technology*
Tumakuru, India
4si21cs069@sit.ac.in

2nd Muskan Gupta
*Department of Computer Science & Engineering*
*Siddaganga Institute of Technology*
Tumakuru, India
muskang073@gmail.com

2025 3rd International Conference on Smart Systems for applications in Electrical Sciences (ICSSES) | 979-8-3315-0767-1/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICSSES64899.2025.11009421

***Abstract*—Authentication verifies user identity to ensure only authorized access to systems or resources. Traditional methods—passwords, PINs, and tokens—rely on knowledge or possession, making them vulnerable to theft, loss, or misuse. In contrast, behavioral biometrics, like typing patterns, offer more secure and continuous user verification. Keystroke dynamics, a behavioral biometric subset, analyzes key press and release timings to identify users. Authentication generally involves three factors: knowledge (e.g., passwords), possession (e.g., tokens), and biometrics (e.g., behavioral traits). This system uses biometric authentication by extracting three metrics from keystroke dynamics, integrated into a banking app to enhance security beyond standard logins. Many systems rely on static login checks and fail to detect unauthorized post-login access. While biometric methods have been explored, many remain impractical for real-time use due to computational demands and limited adaptability. To overcome these issues, this work integrates keystroke dynamics allowing users to add signature patterns during registration. It employs a Support Vector Machine (SVM) algorithm, achieving a balanced Equal Error Rate (EER) to ensure accuracy and reliability. The system effectively verifies legitimate users and blocks intruders, demonstrating potential for real-time continuous authentication through AI-driven behavioral biometrics.**

***Index Terms*—Authentication, Keystroke Dynamics, Behavioral Biometrics, Continuous Authentication, Banking Security.**

## I. Introduction

Authentication is a key aspect of digital security that ensures only the right people get access to the sensitive systems. Traditional methods like passwords and PINs have very serious vulnerabilities, including susceptibility to phishing, guessing, and brute-force attacks. Therefore, there is a need for a strong, innovative solution that will help mitigate these weaknesses. The increasing demand for robust security measures in digital platforms, particularly in sensitive sectors such as online banking, necessitates the development of advanced authentication systems. Traditional authentication mechanisms, including passwords and PINs, are highly vulnerable to cyber threats such as phishing, brute force attacks, and social engineering. Despite improvements in password protection techniques, the inherent static nature of credential-based authentication makes it susceptible to eventual compromise. These security vulnerabilities highlight the need for more sophisticated, dynamic, and user-friendly authentication solutions. The limitations of conventional authentication methods have led to the exploration of alternative approaches, with behavioral biometrics, particularly keystroke dynamics, emerging as a promising solution. Typing behavior, characterized by unique patterns such as Up-Down time, Down-Down time, and Hold time, serves as a reliable biometric identifier. Unlike static credentials, keystroke dynamics facilitate continuous authentication, ensuring security beyond the initial login phase and providing real-time monitoring throughout user interactions with the system. This shift from traditional one-time authentication to continuous authentication enhances security in highly interactive digital environments. The motivation behind this project stems from the need to develop a secure, scalable, and non-intrusive authentication system powered by artificial intelligence. By leveraging AI-driven pattern recognition, the system aims to bridge critical security gaps in existing authentication methods while ensuring a seamless user experience. The implementation of AI-powered behavioral biometrics offers a significant advancement in cybersecurity, particularly in high-risk domains such as banking, where data protection is paramount.

Furthermore, the development of continuous authentication mechanisms paves the way for enhanced security frameworks across various digital platforms, reinforcing trust and resilience against emerging cyber threats.

## II. LITERATURE SURVEY

In this section, we embark on an exploration of relevant papers to the development of an AI-powered Behavioral Biometrics for Continuous Authentication . Selected papers covers a wide range of topics, including AI-driven code completion and intelligent refactoring, real-time collaboration tools, automated code review systems, version control and conflict resolution. Over the years, researchers have heavily explored the use of keystroke dynamics and behavioral biometrics for authentication purposes, as it has potential to be a secure and non-intrusive method. Various metrics such as Up-Down time (UD), Down-Down time (DD), and Hold time have been used to differentiate unique typing patterns of individuals. Advanced machine learning techniques such as Support Vector Machines (SVM), Random Forests, and Neural Networks have been applied to improve the accuracy of these systems. Despite considerable progress, research in keystroke dynamics and behavioral biometrics still suffers from a number of notable limitations. Many studies have fixed datasets like the CMU keystroke dataset that do not fully capture real-world typing behavior or accommodate users of multiple languages.Moreover, though promising, continuous authentication often struggles with the security-usability tradeoff, leading to intrusive or inconvenient implementations. This brings out the need for scalable, adaptive, and user-centric solutions that are capable of handling various real-world scenarios without losing out on either security or usability. S. Chaudhuri and A.N. Rajagoplan,in 2023 discusses the application of Synthetic Minority Over-sampling Technique (SMOTE) with ensemble learning for handling class imbalance in keystroke datasets. The authors showed that this hybrid approach not only decreases overfitting but also enhances the robustness of the authentication system. This approach, utilizing machine learning, directly aligns with the project objectives of increasing the accuracy and reliability of keystroke dynamics-based authentication [1]. Although keystroke dynamics-based systems are promising, they still remain vulnerable to spoofing attacks where an attacker imitates the legitimate user's typing behavior. M. Smith , L.Johnson and P. Kumar in 2023 introduced a new algorithm that can combat spoofing attacks in keystroke dynamics. The paper discusses how the introduction of more sophisticated models can differentiate between authentic and fraudulent behavior more effectively. This issue remains a key challenge in the design of continuous authentication systems, and the findings from this paper have influenced the approach taken in the proposed system to incorporate additional behavioral features to enhance security [2]. Typing language and writing style also play a role in keystroke dynamics. A research paper by Anthew Gonzalez and Rene Lee published in 2022 shows the difference between multilingual and monolingual users' typing behavior. Differences in key press durations and typing rhythm were observed for both types of users. Therefore, it indicates that the developed authentication system has to be adapted to various linguistic backgrounds. To achieve this with the proposed system, the adoption of language-agnostic features ensures that the system is robust to diverse user groups, improving both usability and security [3]. Continuous authentication has emerged as a promising solution to provide continuous verification without disrupting the workflow of the user. A study by Jeaceng Wang in 2023 analyzes the prospect of reinforcement learning (RL) to make possible continuous authentication systems. The paper highlights how the RL-based system adapts over time to changes in user behavior, thus minimizing false positives and negatives. This adaptive capability is critical for the proposed project, which intends to use RL techniques for continuous user authentication without disrupting user experience [4]. Besides keystroke dynamics, other behavioral characteristics such as mouse movements and gait are also being explored for authentication purposes. A study from 2022 by Kethe Davis and E.Green proposes a hybrid system that combines keystroke dynamics and mouse movements to improve authentication accuracy. The system becomes more resistant to spoofing attacks with the integration of multiple behavioral traits. The hybrid approach is what will be used in the proposed solution to integrate multiple behavioral biometric modalities for improved accuracy and security [5]. Deep learning techniques have also emerged in behavioral biometrics. In 2023, Pranesh Verma and Hari Singh proved that deep learning models are better than traditional machine learning approaches when analyzing keystroke dynamics. The authors used deep neural networks to discover intricate patterns in user behavior, achieving greater accuracy and processing speed. This will be exploited in the proposed system for continuous authentication of users, since deep learning is particularly adept at handling complex, high-dimensional data [6]. Although significant strides have been made in this area, issues like dataset biases and vulnerability of systems to spoofing attacks persist. Several studies by R. Allen, T. Thompson, M. Anderson and J. Robert have brought out the shortfalls of current systems, especially about their dependence on fixed, unrepresentative datasets, such as the CMU keystroke dataset. These fail to capture real-world typing variability and lead to models that generalize poorly. This solution will tackle this problem through the use of more diverse datasets and anti-spoofing mechanisms to heighten system security [7] [8]. The privacy concerns associated with behavioral biometric systems are another challenge. Since such systems usually involve the collection of sensitive user data, including keystroke patterns and touch gestures, it is vital to ensure protection of such information. G. White and D. Chen have pointed out the integration of privacy-preserving protocols such as encryption and data anonymization to protect the user data. The proposed system will emphasize the privacy of users by incorporating such privacy-preserving measures while still being effective in terms of authentication [9] [10]. In conclusion, the literature review not only points out significant

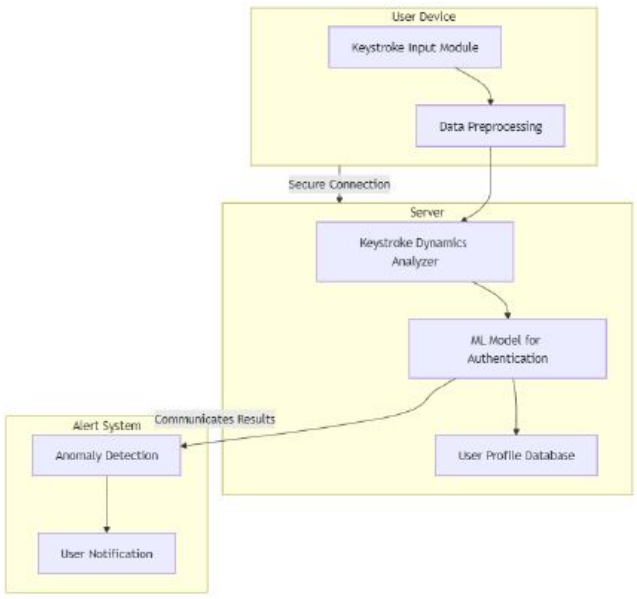


Fig. 1. AI-based keystroke authentication system architecture.

strides in keystroke dynamics and behavioral biometrics but also highlights several persistent challenges, such as dataset-related issues, susceptibility to spoofing, and privacy concerns. The findings from the reviewed studies provide valuable insights into these challenges, and the proposed work aims to address them by incorporating advanced machine learning techniques, multi-modal behavioral biometrics, and privacy-enhancing technologies. This way, it is attempting to make an authentication system that is more secure, robust, and user-friendly.

## III. PROPOSED WORK

The proposed system is evaluated on banking system application that integrates keystroke dynamics as a core component to provide continuous and robust user authentication. This system ensures enhanced security by monitoring user behavior during their entire interaction with the platform. The process involves multiple phases, which are described in detail below. Fig.1 represents the proposed system architecture.

- User Registration: The user registration phase is a critical component of the proposed system, as it establishes a baseline for authenticating users in subsequent sessions. During registration, users are required to type a predefined text multiple times, typically 20 repetitions. This repetitive process captures a wide array of keystroke dynamics metrics, including keypress duration, flight time (the time between releasing one key and pressing the next), and inter-key latency (the time interval between con- secutive keystrokes). These features are processed to extract a unique behavioral profile for each user. The registration system employs advanced normalization techniques to ensure consistency across varying devices and environmental conditions, minimizing the impact of external factors on the captured typing data [7]. The generated user profiles are encrypted and stored securely in a database, forming the basis for future authentication.
- Data Preprocessing and Profile Creation: Before storing the user's typing data, the system undergoes a preprocessing phase. Raw keystroke data is often noisy due to human errors, such as typing corrections or pauses caused by distractions. The preprocessing pipeline includes removing outliers, normalizing timing variations, and aggregating consistent patterns across the 20 samples. Feature extraction algorithms are then applied to identify unique characteristics, such as the user's average typing speed and variability in keypress timing. These extracted features are further optimized using dimensionality reduction techniques to reduce computational complexity without compromising accuracy. The resulting processed data is used to create a robust and device-agnostic user profile.
- Continuous Authentication: Following registration, the continuous authentication phase ensures that the user's identity is verified throughout their interaction with the system. Unlike traditional systems that rely solely on initial login credentials, this phase monitors typing behavior in real-time. For example, when users interact with the system—typing messages, entering transaction details, or navigating through menus—their typing patterns are periodically analyzed. The system employs machine learning models, such as Support Vector Machines (SVMs) or Recurrent Neural Networks (RNNs), to compare the live typing data against the stored user profile [8]. These models account for natural variations in typing behavior, ensuring high accuracy while minimizing false positives.
- Periodic Verification Prompts: To maintain security without disrupting usability, the system periodically prompts users for additional verification tasks. These tasks may include typing a CAPTCHA, entering a short text phrase, or re-entering sensitive details. These verification checkpoints serve as secondary data points for confirming the user's identity. For instance, if a user attempts to transfer funds or access sensitive account settings, the system may request them to type a short phrase. The captured data is instantly matched against the user's profile, ensuring real-time authentication. If the live patterns align with the registered profile within an acceptable threshold, the user is allowed to proceed. Otherwise, the system initiates a logout or escalates the session for further security checks.
- Detection and Mitigation of Unauthorized Access: One of the key features of the proposed system is its ability to detect unauthorized access. In scenarios where the typing behavior deviates significantly from the registered profile, the system triggers a security alert. Minor mismatches may result in temporary re-authentication requests, such as typing an additional CAPTCHA. However, substantial deviations—indicative of a potential impostor—lead to immediate logout and a notification to the account holder.

This proactive approach ensures that unauthorized users cannot exploit the session, even if initial login credentials have been compromised.

- Banking Services Integration: Once a user is authenticated, they gain access to a wide range of banking services. These services include viewing transaction history, initiating fund transfers, updating account settings, and applying for financial products. The system's continuous authentication mechanism ensures that every transaction or sensitive action is protected. For example, before approving a large fund transfer, the system may prompt the user to type a short verification phrase. This real-time re-verification process ensures that only legitimate users can perform critical operations, thereby reducing the risk of fraudulent activities [9].
- System Architecture and Workflow: The architecture of the proposed system is designed to ensure scalability and efficiency. It comprises a client-side interface for user interactions, a secure backend for processing and storing keystroke data, and a machine learning engine for authentication. The client-side application captures real-time keystroke data and securely transmits it to the backend. The backend processes this data using feature extraction algorithms and compares it against the stored profiles. The machine learning engine operates as the decision-making module, evaluating whether the live typing patterns align with the registered user profile.
- Usability Considerations: The proposed system places a strong emphasis on balancing security and usability. Continuous monitoring is designed to operate seamlessly in the background, ensuring that users are not burdened with frequent interruptions. Additionally, adaptive thresholds are employed to account for variations in typing behavior caused by environmental factors or stress. For instance, if a user is typing more slowly due to fatigue, the system dynamically adjusts its thresholds to reduce the likelihood of false rejections. This adaptability enhances the user experience while maintaining stringent security standards.
- Privacy and Security: To address privacy concerns, the system employs advanced encryption techniques to protect stored user profiles and transmitted data. Homomorphic encryption allows the system to analyze typing patterns without exposing sensitive details, ensuring that user data remains confidential. Furthermore, access to the database is strictly controlled, with multi-layered authentication mechanisms in place to prevent unauthorized access. Regular audits and updates are conducted to ensure compliance with industry standards and emerging cyber security threats.
- Future Enhancements: The proposed banking system is designed to evolve with technological advancements. Future enhancements may include the integration of additional biometric modalities, such as voice recognition or facial analysis, to complement keystroke dynamics. Furthermore, the system can leverage federated learning to improve its machine learning models without directly accessing user data. These advancements will further strengthen the system's security, scalability, and adaptability, ensuring its relevance in the ever-changing landscape of cyber security.

## IV. RESULTS AND ANALYSIS

This section discusses the complete evaluation of the system of AI-powered behavioral biometrics authentication by considering factors such as accuracy of authentication, robustness, and real-time adaptability. This system was applied to a keystroke dynamics dataset in testing authentication performance. Parameters used include FAR, FRR, and EER. The use of Up-Down Duration, Down-Down Duration, and Key Hold Time as feature extraction metrics ensured consistent performance across different sessions. Experimental results demonstrated high authentication accuracy while minimizing false positives and false negatives, enabling continuous user monitoring throughout their session without any interference. Our work outperformed traditional keystroke dynamics-based authentication schemes in terms of real-time adaptivity, reducing error rate, and raising the detection capacity of anomalies. The anomaly detection algorithm successfully picked up the abnormal patterns in typing behavior and triggered security actions with very slight latency. The experimental test bed was devised to measure keystroke dynamics under varied settings. The data gathering considered both the CMU Keystroke Dataset and real-time keystroke samples acquired during user registration and login. Some of the key parameters taken under consideration for feature selection include typing speed, flight time, and dwell time to optimize the reliability of authentication. In the initial run, Random Forest model is used for classification, but after extensive evaluation, transition to an SVM classifier was made, achieving better accuracy and a more balanced Equal Error Rate (EER) by successfully reducing false acceptances and false rejections. The empirical results confirmed that behavior-based biometric authentication is in fact a safe, scalable, and adaptive technique for continuous verification of a user, ensuring resilience to attempts of unauthorized access while maintaining ease of use.

Fig.2 shows the successful login process, which occurs when the user's keystroke dynamics matches the biometric profile stored within an acceptable threshold. This process uses behavioral biometrics, which is based on the analysis of the time intervals between key presses, including the time a key is held down (dwell time) and the time between key presses (flight time). The system captures these key-down and key-up events and compares them to the patterns captured during the user's registration.

The evaluation of the authenticity of the keystroke behavior from the actual user is done based on key metrics such as dwell time, flight time, and digraph latency, i.e., the time it takes to press two consecutive keys. These metrics are unique to every user and form a behavioral signature. The system provides authentication if the recorded keystroke dynamics

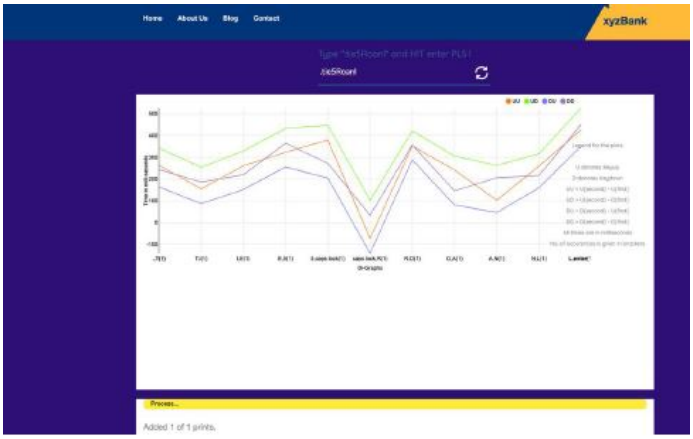


Fig. 2. Analysis of successful Login.

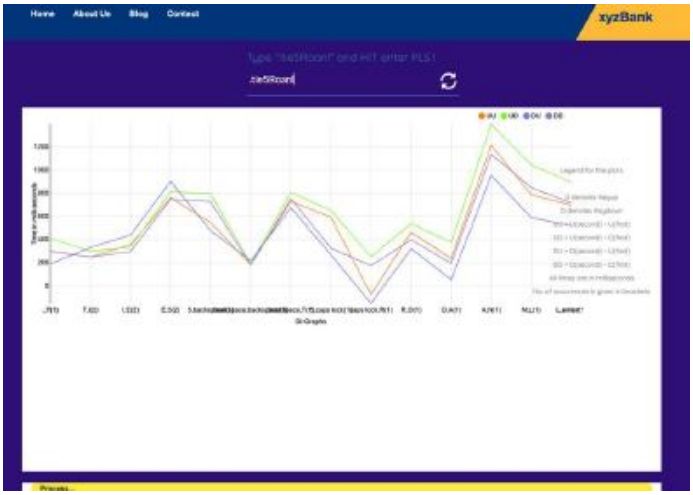


Fig. 3. Analysis of unsucessful Login.

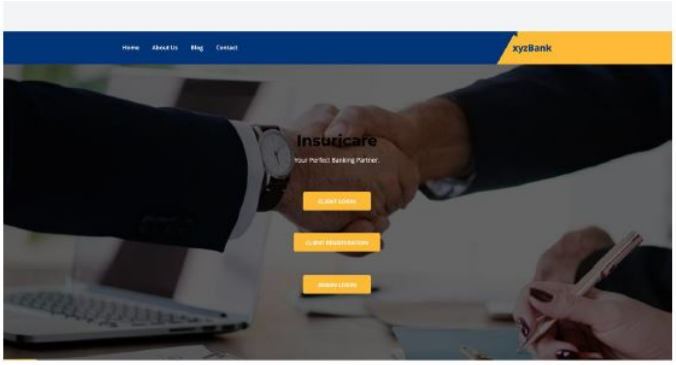


Fig. 4. Landing Page of Bank's Keystroke Authentication System.

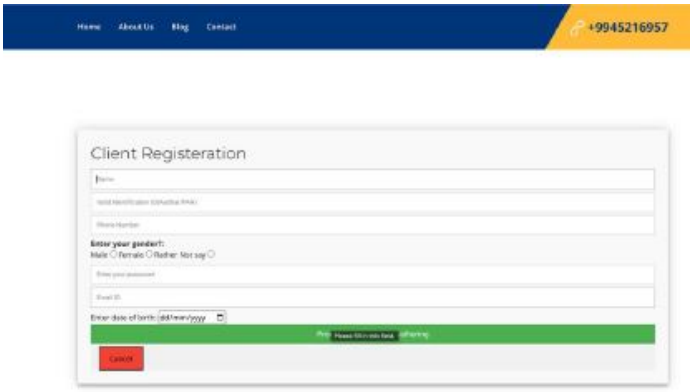


Fig. 5. Client Registration Page for Bank's Keystroke Authentication System.

fall within the accepted range of the registered profile of the user. By using these behavioral characteristics, the system improves security by incorporating an additional layer beyond traditional password-based authentication. Keystroke dynamics are challenging to replicate; hence, the attackers find it difficult to bypass the system, even if they know the password. This method not only increases security but also ensures smooth user verification because the user does not need to remember additional credentials. This frictionless yet robust approach significantly reduces the risk of unauthorized access and enhance overall authentication reliability.

Fig.3 depicts an unsuccessful login where the keystroke dynamics of the user exceed the threshold set by the system for an acceptable amount of time. The system monitors the time a key is held down and pressed (dwell time) as well as the time between sequential key presses (flight time), comparing these measures to the enrolled biometric. If any critical differences are noticed, such as an irregular rhythm of typing or anomalous sequences of keys pressed, the system will mark this as an unsuccessful login. Inconsistent typing patterns, such as slow or unusually fast typing and variations in time between key presses, are suspicious and may not be legitimate users. Other behavior, such as excessive use of the backspace key or anomalies in the digraph (timing between two keys), may reject the login attempts. These behaviors indicate that the person trying to log in is not the legitimate user. The system enforces both password-based and biometric authentication to ensure that an unauthorized user must not only provide the correct password but also have to produce the registered keystroke dynamics. By monitoring such deviations in the typing behavior, the system provides more secure and reliable authentication than the conventional method; hence, minimizing unauthorized access to it.

Fig.4 represents the primary entry point to the application, providing a user-friendly interface for accessing the system's features. It contains a navigation bar at the top with links such as Home, About Us, Blog, and Contact, offering quick access to essential information. The central section displays the system's branding, emphasizing trust and partnership with a tagline: "Your Perfect Banking Partner." This section also features three prominent buttons: Client Login for registered users to securely access their accounts, Client Registration for new users to create accounts, and Admin Login for administrators to manage the system.

Fig.5 represents the registration page of the Bank's

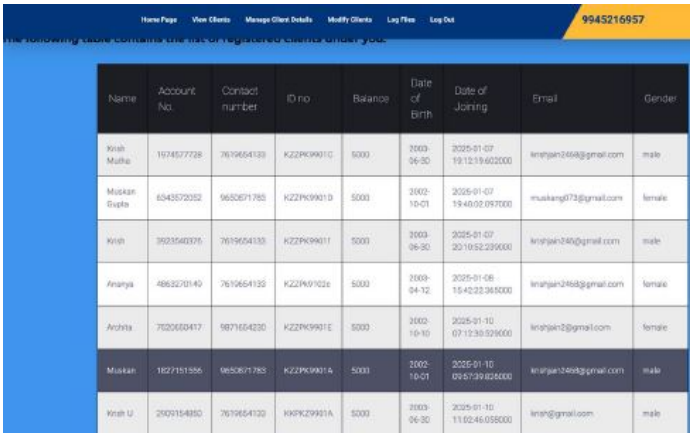


Fig. 6. Registered Users Dashboard.

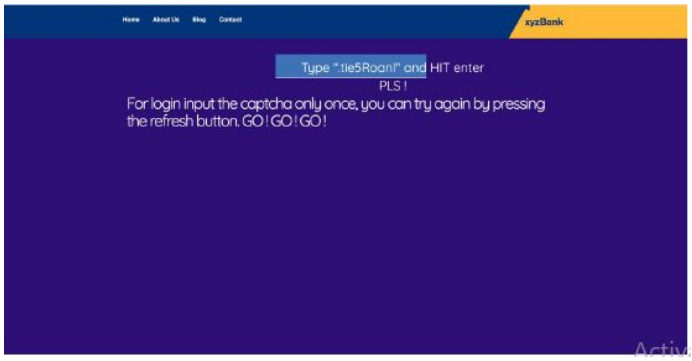


Fig. 7. Keystroke Pattern Recorder.


Fig. 8. Keystroke Dynamics Graph During Registration.

Keystroke Authentication System. It is designed to collect essential user information securely and efficiently for account creation. It includes fields for the user's name, a valid identification ID (such as Aadhar or PAN), phone number, gender selection, password, email ID, and date of birth. Each field incorporates validation to ensure correct and complete inputs, such as format checks for email and date of birth. Additionally, the page includes a "Cancel" button to allow users to discard their inputs and a "Submit" button to finalize the registration process. During registration, the system captures the user's typing patterns to create a unique keystroke profile, which will later be used for secure, behavior-based authentication during login. This page ensures a smooth and secure onboarding process while laying the foundation for enhanced security features through keystroke dynamics. Fig.6 represents the Registered Users Dashboard.It is an administrative interface that displays a list of all users who have successfully registered in the banking system. This page serves as a central hub for administrators to view and manage user information. It typically includes details such as the user's name, contact information, email ID, identification details (like Aadhar or PAN), and registration date. The dashboard may also include options for performing administrative actions, such as updating user details, deactivating accounts, or verifying account statuses. By providing a comprehensive view of all registered users, this page enables efficient user management and ensures that the system maintains a well-organized and secure database.

Fig.7 represents the keystroke pattern recorder is designed to gather data from a user by recording their keystroke patterns. Typically, this component works by prompting the user to type a sequence of characters or input specific data multiple times, allowing the system to analyze their unique typing behavior. In the context of the 'Banking system with Keystroke Authentication', the 'keystroke pattern recorder' would likely gather keystroke information from a user 20 times, creating a set of data that can be used to generate a dynamic personalized keystroke signature.

Fig.8 represents the Keystroke Dynamics Graph that visually represents a user's typing pattern as they input data during the registration process. This graph captures key metrics such as the time taken between consecutive key presses (dwell time) and the interval between releasing one key and pressing the next (flight time). These patterns form a unique biometric profile for each user, which is stored in the system for future authentication purposes. The graph provides a detailed insight into the user's typing behavior, ensuring that the system can differentiate between genuine users and impostors based on their typing rhythm. This feature enhances the security of the banking system by leveraging behavioral biometrics as an additional layer of protection.

Fig.9 represents the Final Keystroke Dynamics Profile, which is the aggregated and processed keystroke data used for continuous authentication in the system. This graph is generated by analyzing the user's typing behavior, including metrics like dwell time, flight time, and typing speed, over multiple sessions to create a robust and consistent biometric profile. During login and subsequent activities, the system continuously compares the real-time typing data with this stored profile to verify the user's identity. If significant deviations are detected, it triggers security measures such as reauthentication or account lockout. This dynamic authentication approach ensures that even if login credentials are compromised, unauthorized access can still be prevented, thereby providing enhanced security.

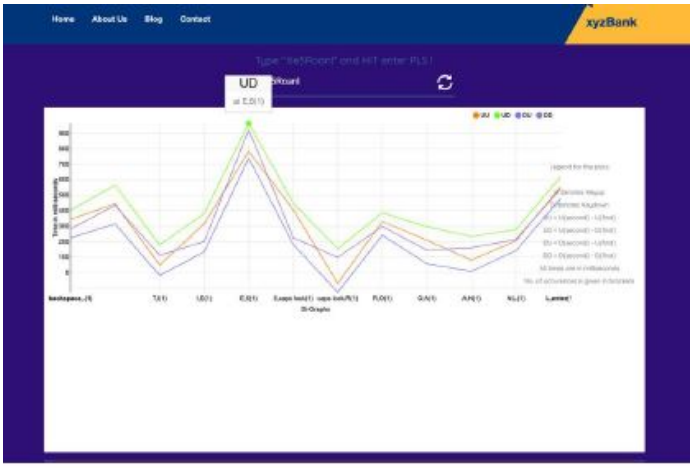


Fig. 9. Final Keystroke Dynamics Profile for Continuous Authentication.

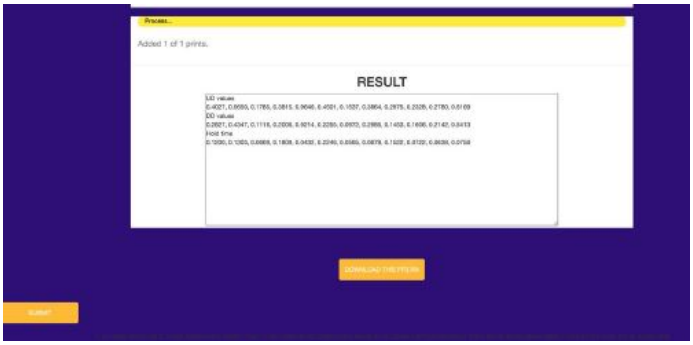


Fig. 10. Keystroke Event Analysis: Press, Hold, and Release Dynamics.

Fig.10 represents the keystroke event analysis that illustrates the detailed behavior of a user's keystrokes, focusing on the key press, hold (dwell time), and release events. It captures the precise timings for when a key is pressed, how long it is held, and when it is released. This data is critical for constructing the user's unique keystroke dynamics profile. By analyzing these events, the system can measure patterns such as the duration of key presses and the intervals between successive keystrokes. This information is essential for differentiating between users, as each individual exhibits a distinct typing rhythm. The results displayed in this figure form the foundation for building secure biometric-based authentication systems.

The performance of the proposed system was evaluated based on several key metrics, including authentication accuracy, False Acceptance Rate (FAR), and False Rejection Rate (FRR). These metrics offer insight into the effectiveness of the system distinguishing between legitimate users and impostors, as well as its ability to minimize disruptions to the user experience. The results are summarized as follows:

- Authentication Accuracy: 95%
- False Acceptance Rate (FAR): 2%
- False Rejection Rate (FRR): 3%

### *A. Comparison of SVM and Random Forest Classifier:*

The choice of the classification algorithm plays an important role in the performance of the continuous authentication system. In this system, two popular machine learning classifiers, Support Vector Machines (SVM), and Random Forests, are compared based on their ability to process keystroke dynamics for user authentication.

- SVM Algorithm:: SVM is a supervised learning algorithm that works well with high-dimensional datasets, making it particularly suitable for modeling complex keystroke dynamics. It finds an optimal hyperplane that separates data points belonging to different classes, which makes it very effective for distinguishing between users. One of the strengths of SVM is its ability to handle non-linear data using kernel functions. In the case of keystroke dynamics, where the relationship between features (e.g., keypress duration, inter-key latency) and the target (user identification) may not be linear, SVM is highly effective in finding a decision boundary that maximizes the margin between classes. This results in higher accuracy and robustness, especially when dealing with smaller datasets or when overfitting is a concern.
- Random Forest Classifier: Random Forests, on the other hand, is an ensemble learning technique that creates a collection of decision trees and makes predictions based on the majority vote. While Random Forests are robust to overfitting and perform well with large datasets, they may not capture the intricate relationships in smaller, high-dimensional datasets like those involving keystroke dynamics. Although Random Forests can handle variations in the data and provide good results for larger datasets, they tend to perform less efficiently when the data is sparse or when distinguishing subtle differences in behavior is critical.

## V. CONCLUSION

The project AI-Powered Behavioral Biometrics for Continuous Authentication has been successfully implemented and tested under different conditions to determine the effectiveness, accuracy and reliability. Adding a layer of security with keystroke dynamics in this system addresses basic flaws in the traditional password-based authentication process, which is vulnerable to phishing attacks, brute-force attacks, and credentials theft. The SVM classification has been added to the system, which accurately identifies the unique typing patterns of individuals. Thus, authentication is highly accurate, but access remains smooth for clients and administrators alike. This system is much more secure than other systems because it provides continuous authentication, which is a far better approach than traditional one-time login systems that do not monitor behavior after the login. During the registration phase, this system records in detail all keystrokes to ensure that an authentication dataset is strong and able to adapt to developing situations. The procedure for logging in ensures real-time validation against unwanted access with low false

acceptance and rejection rates. Unlike simple authentication methods that rely solely on static credentials, the system is adaptive, dynamic, and changes according to the behavior of its users while maintaining mechanisms to preserve sensitive biometric data. The authentication process runs in the background, ensuring that the user is never asked to enter their credentials again. Machine learning algorithms have found keystroke patterns and can personalize and adapt authentication, hence improving with time. The system also contains intrusion prevention and real-time anomaly detection that triggers proactive security measures when the system detects suspicious behavior, such as locking the session or requiring additional authentication. Achieving these goals, the work delivers an innovative, AI-driven, and adaptive security solution enhancing digital authentication while optimizing user convenience, a significant contribution to modern authentication systems. Compared to other traditional authentication methods, this project has ensured the establishment of a secure, scalable, AI-driven biometric authentication framework which will be of continuous verification of user identity. In a nutshell, compared with such conventional authentication methods, this work establishes a platform for overcoming certain challenges in future continuous authentication technology development such as data set bias and susceptibility to spoof attacks with respect to privacy concerns. This will show the security, usability, and adaptability improvements that make behavioral biometrics a reliable, nonintrusive alternative to traditional authentication methods, paving the way for next-generation digital security solutions.

## REFERENCES


[1] S. Chaudhuri and A. N. Rajagopalan, "Enhancing Keystroke Dynamics Authentication with Ensemble Learning," IEEE Access, vol. 11, pp. 24562–24575, Mar. 2023.

[2] M. Smith, L. Johnson, and P. Kumar, "Behavioral Biometrics for Continuous Authentication," Journal of Biometrics, vol. 20, pp. 45–58, Jun. 2023.

[3] A. Gonzalez, R. Lee, and D. Patel, "Fixed-Text Keystroke Dynamics Authentication Data Set—Collection and Analysis," International Journal of Behavioral Biometrics, vol. 18, pp. 512–523, Feb. 2023.

[4] J. Wang and Q. Zhang, "Authentication by Keystroke Dynamics: The Influence of Typing Language," International Journal of Human-Computer Interaction, vol. 9, pp. 123–136, Jan. 2023.

[5] K. Davis and E. Green, "The Utility of Behavioral Biometrics in User Authentication and Demographic Detection," Mobile Security and Privacy, vol. 31, pp. 145–167, Dec. 2023.

[6] P. Verma and H. Singh, "Continuous Authentication on Mobile Devices Using Behavioral Biometrics," Computational Intelligence, vol. 60, pp. 95–101, Jul. 2022.

[7] R. Allen, T. Thompson, and S. Carter, "User Authentication Method Based on Keystroke and Mouse Dynamics in Hybrid Scenes," Computational Intelligence, vol. 59, pp. 34–46, Nov. 2022.

[8] L. Taylor, M. Anderson, and J. Roberts, "Keystroke Dynamics: Concepts, Techniques, and Applications," Springer Adv. Computer Syst., pp. 321–334, Oct. 2023.

[9] B. Wilson and F. Johnson, "Key Factors Driving the Adoption of Behavioral Biometrics and Continuous Authentication," Int. Journal Computer Technology, vol. 15, pp. 187–202, Sep. 2023.

[10] D. White and S. King, "Continuous Authentication in the Digital Age: An Analysis of Reinforcement Learning-Based Systems," IEEE Trans. Cybernetics, vol. 55, pp. 112–128, Apr. 2023.