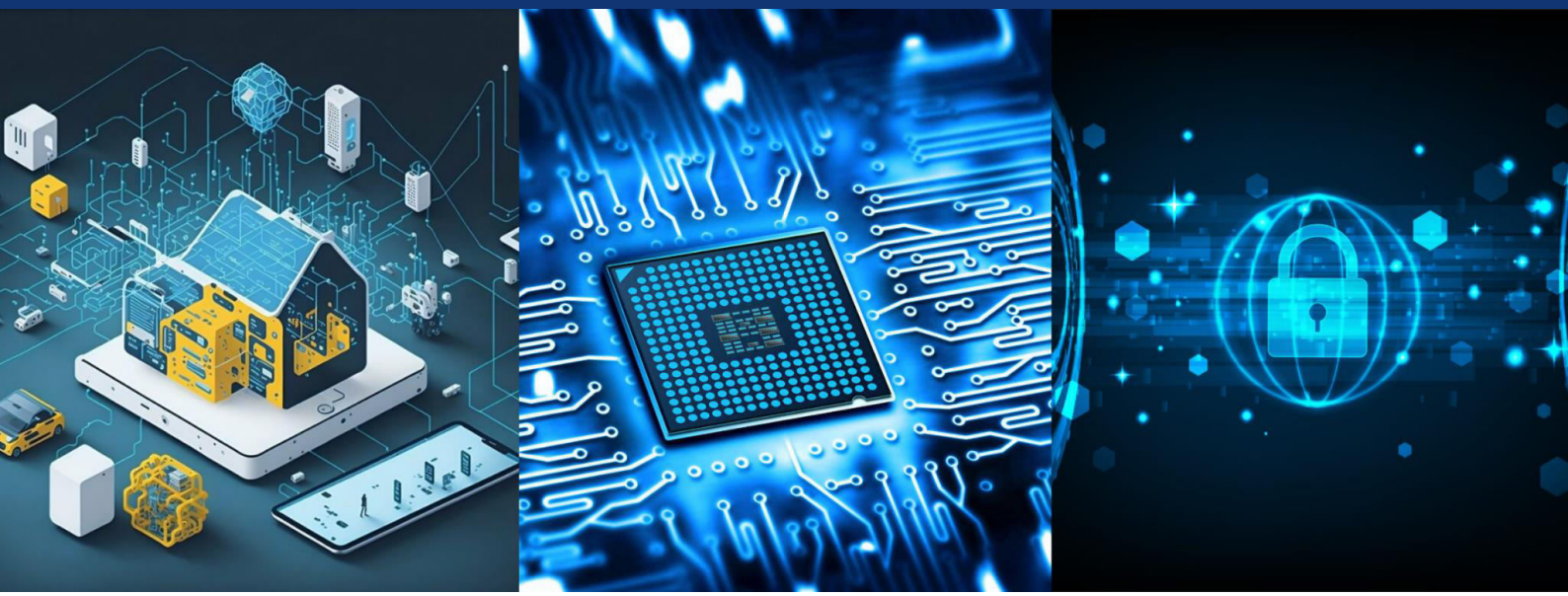
IJIRCCE

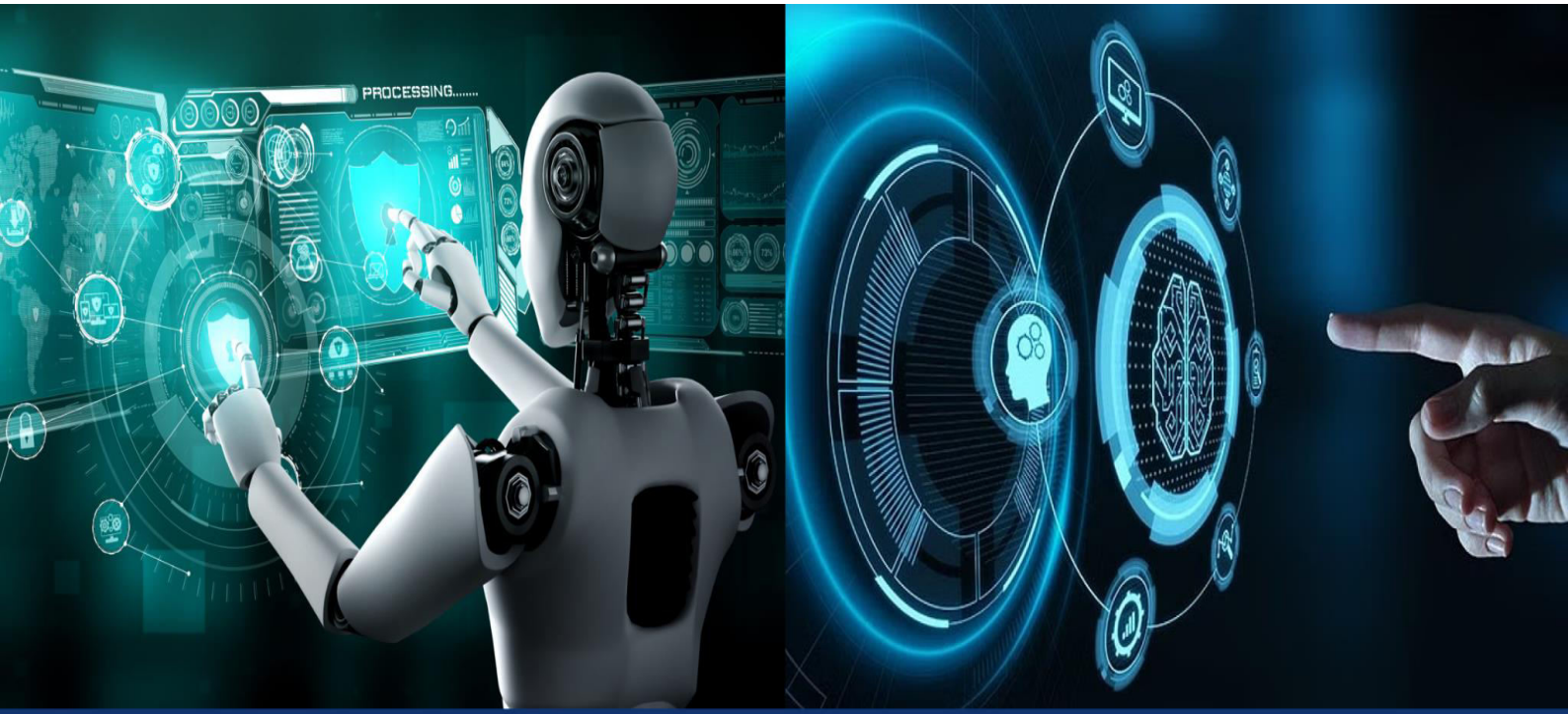
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.927

Volume 14, Issue 6, June 2026

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406107

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Sapien AutheiX: AI-Based Continuous Authentication Using Keystroke Dynamics for Behavioral Biometric Security

Bingi Pallavi[1], Surampalli Balakrishna[1], M. Lakshmi Aparna Bhukta[1], M. Ashfaque Afridi[1], Dr. J. Aruna Devi[2]

Department of Computer Science and Engineering (DS), Anil Neerukonda Institute of Technology and Sciences, Visakhapatnam, India[1]

Associate Professor, Department of Computer Science and Engineering (DS), Anil Neerukonda Institute of Technology and Sciences, Visakhapatnam, India[2]

ABSTRACT: The success of continuous authentication systems based on behavioral biometrics has gained importance due to the limitations of traditional authentication methods. This work proposes a lightweight AI-based authentication system that identifies users in real-time using keystroke dynamics. Unlike multi-modal biometric systems, the proposed framework focuses on efficient feature extraction using keystroke timing elements such as dwell time and flight time. The sys-tem employs a combination of XGBoost, Support Vector Machine (SVM), and Hidden Markov Model (HMM) to achieve accurate and low-complexity authentication. Additionally, a USB or digital key-based fallback mechanism is introduced to prevent user lockouts. Experimental results demonstrate that the proposed system achieves reliable performance with reduced computational cost, making it suitable for real-time applications.

KEYWORDS: Behavioral Biometrics, Keystroke Dynamics, Continuous Authentication, XGBoost, SVM, HMM, Lightweight AI, Cybersecurity

I. INTRODUCTION

Conventional authentication systems verify a user's identity only at login and assume the same per-son continues using the system, which creates security risks. Behavioral biometrics addresses this issue through continuous authentication, where user activity is monitored throughout the session. Keystroke dynamics is an effective method as it is non-intrusive and does not require additional hardware. Typing patterns, influenced by coordination and habits, are consistent enough to distin-guish genuine users from impostors.

Earlier approaches relied on statistical features such as key press duration and inter-key inter-vals. Although simple to implement, these methods were sensitive to variations in typing behavior caused by factors like fatigue, leading to reduced accuracy. Machine learning and deep learning techniques have improved performance; however, they often require large datasets, high computa-tional resources, and frequent retraining, making them less suitable for real-time systems.

To address these limitations, this work proposes a lightweight continuous authentication system using keystroke dynamics. The system combines XGBoost, Support Vector Machine (SVM), and Hidden Markov Model (HMM) to capture both pattern-based and sequential behavior. It supports real-time monitoring to detect anomalies and trigger security responses, along with a USB or digital key-based fallback mechanism to prevent lockouts.

II. RELATED WORK

Behavioral authentication is a form of biometric authentication that has gained attention as an alternative to traditional static authentication methods. Among various behavioral characteristics, keystroke dynamics is widely used due to its non-intrusive nature and no requirement for additional hardware. Typing features such as key press timing can differentiate

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406107

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

between genuine users and im-postors using machine learning algorithms, as demonstrated by Harun et al. [2]. Keystroke-based authentication has also been applied to mobile environments using dimensionality reduction techniques such as Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA), showing reliable identification even with limited data [3]. More advanced approaches use deep neural networks, including convolutional and recurrent architectures with attention mechanisms, to improve classification accuracy [4]. Continuous authentication systems based on keystroke bi-gram features and neural networks have also been explored for free-text verification [5]. Systems analyzing mouse interaction patterns have shown promising results [6], with low False Acceptance Rate (FAR) and False Rejection Rate (FRR) achieved using classifiers such as Support Vector Ma-chines (SVM) and Artificial Neural Networks (ANN) [7]. These methods can operate in real-time even with limited mouse events [8]. Continuous authentication frameworks using natural mouse movements and one-class SVM have also been proposed [9]. However, vulnerabilities such as adversarial mouse paths have been identified [10], and comparative studies of different classifiers highlight varying performance levels [11]. Recent studies emphasize deep learning models such as CNN, LSTMs, and GRUs for capturing spatial and temporal features to enhance authentication [12], [15]. Despite their effectiveness, these models are computationally expensive. In contrast, the proposed Sapien AutheiX framework utilizes a lightweight ensemble approach based on keystroke timing characteristics to achieve efficient and accurate continuous authentication.

III. DATASET AND FEATURE REPRESENTATION

A. Data Collection Framework

Behavioral data is collected using a customized keystroke logging module that records fine-grained data during natural typing. Unlike controlled experiments where predefined text is used, this ap-proach captures realistic user behavior, aligning with continuous authentication paradigms.

For each keystroke event, the system records:

- Key code (ASCII or virtual key identifier)
- Key press timestamp
- Key release timestamp

Timestamps are recorded in milliseconds to ensure sufficient resolution. Logging is performed asynchronously, introducing negligible latency and preserving behavioral accuracy.

TABLE I

RAW DATASET STRUCTURE COLLECTED FROM KEYSTROKE LOGGER

Column Name	Description	Unit
key code press timestamp release timestamp	ASCII / Virtual key code Time at which key is pressed Time at which key is released	Integer milliseconds milliseconds

The dataset consists of typing sessions segmented into fixed-length behavioral windows, where each window represents a sample for authentication.

B. Statistical Characterization

The variability reflects differences in typing speed and behavior among users. Despite intra-user variation, inter-user differences remain distinguishable, enabling effective classification.

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406107

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

TABLE II

STATISTICAL SUMMARY OF EXTRACTED FEATURES

Feature	Mean (ms)	Std Dev	Min	Max
Dwell Time	93.34	136.45	15.60	1835.98
Flight Time	109.87	432.05	-1754.46	4409.47

The dataset remains simple yet discriminative, allowing efficient computation while preserving behavioral individuality through core temporal features and systematic preprocessing.

The proposed authentication system is designed as a lightweight continuous verification framework based on keystroke dynamics. Unlike multi-modal architectures that rely on high-dimensional feature fusion and deep neural networks, this model focuses on efficient temporal modeling and ensemble-based decision fusion, ensuring computational feasibility with strong discriminative per-formance.

A. System Architecture Overview

The authentication pipeline consists of four stages: keystroke event acquisition, feature extrac-tion and preprocessing, ensemble-based classification, and real-time monitoring with decision re-sponse. Each stage is optimized to minimize inference latency and support real-time scalability.

B. Behavioral Window Modeling

Continuous authentication evaluates typing behavior by grouping dwell and flight features into sliding behavioral windows. Let:

$W_j = \{X_j, X_{j+1}, \ldots, X_{j+n}\}$
where $X_i = [Dwell_i, Flight_i]$.
This approach reduces keystroke noise and captures short-term typing rhythm consistency.

C. Real-Time Monitoring Strategy

Continuous authentication requires periodic evaluation of user behavior. A sliding window mech-anism is used, where consecutive windows below the threshold indicate suspicious activity. This approach avoids abrupt lockouts while enabling dynamic behavioral verification.

D. Computational Efficiency Considerations

The framework uses only two temporal features, reducing model complexity. The ensemble oper-ates efficiently on standard CPU-based systems, avoiding the high memory and GPU requirements of deep learning models, making it suitable for enterprise and resource-constrained environments.

IV. RESULTS AND DISCUSSION

The results show that the ensemble-based approach outperforms individual classifiers across all evaluation metrics.
Table 1: Model Performance Comparison

Model	Accuracy (%)	FAR (%)	FRR (%)
XGBoost	94.2	3.1	2.7
SVM	92.8	4.0	3.5
HMM	91.6	4.5	3.9
Proposed Ensemble	96.3	2.1	1.8

The ensemble model achieves 96.3% accuracy with lower FAR and FRR than standalone classi-fiers, showing improved robustness to typing variability.

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406107

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

4.1 Equal Error Rate (EER) Analysis

Equal Error Rate (EER) occurs when FAR equals FRR, and the ensemble shows lower EER than individual models.

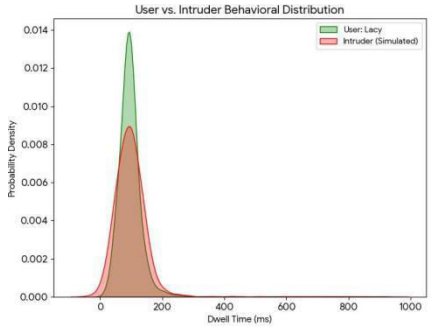
4.2 ROC Curve Interpretation

Receiver Operating Characteristic confirms classifier performance. Ensemble models show a stronger ROC curve and higher AUC than single models, indicating better discriminative power.

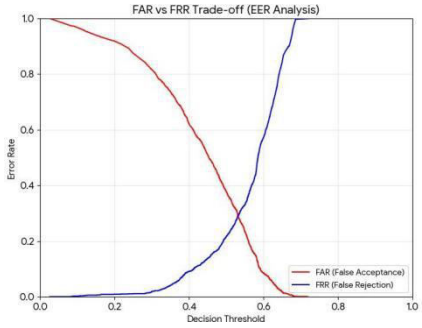
4.3 Confusion Matrix Interpretation

The confusion matrix includes:

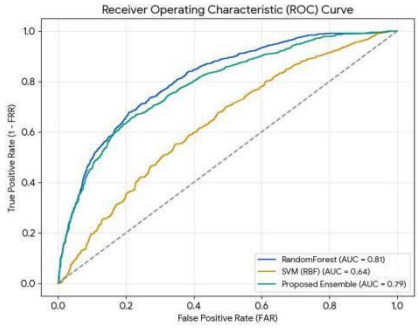
- True Positive (TP): Legitimate user correctly authenticated
- True Negative (TN): Impostor correctly rejected
- False Positive (FP): Impostor incorrectly accepted
- False Negative (FN): Legitimate user incorrectly rejected



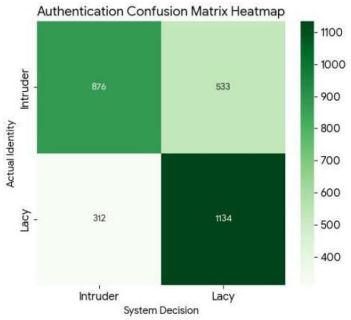
(a) User vs. Intruder Behavioral Distribution Based on Dwell Time



(b) FAR vs FRR Trade-off Curve Showing Equal Error Rate (EER)



(c) Receiver Operating Characteristic (ROC) Curve Comparing Classifiers



(d) Confusion Matrix for Proposed Continuous Authen-tication Model

Figure 1: Performance Evaluation of Proposed Authentication Model

V, SECURITY MECHANISM AND ESCAPE AUTHENTICATION

Continuous authentication systems must have tradeoff between their security and usability. Detec-tion of behavior anomaly is not as vulnerable to unauthorized access and session hijacking but with very high threshold can deny a legitimate user. In this way, a reactive system of security response is incorporated.

Its behavioral windows will give it a curtailed reaction consisting of lock out of the session or even through a sequence of behavioral windows which are beneath the authentication level. In lieu of terminating the session, it offers a little check-up time to reduce the disturbance with temporary typing variations.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

It has a backup escape authentication system to avoid a lockout. A permitted USB key or digital authentication token is an override element, which permits one to re-establish the session without complete re-authentication. It is less dangerous and more comfortable to a user and it is a bi-layered one.

VI. CONCLUSION AND FUTURE WORK

Sapien AutheiX is a lightweight authentication system based on keystroke dynamics. Unlike computationally-intensive multi-modal and deep learning models, it uses temporal features such as dwell and flight time with XGBoost, SVM, and HMM classifiers at low computational cost. The ensemble balances discriminative classification and temporal modeling with low FAR and FRR, supported by an active tracking system and a USB/digital key-based escape mechanism for improved security and usability.

Future work includes adaptive threshold optimization for context-based authentication, along with exploring additional behavioral modalities such as mouse dynamics or touch interaction, and im-proving cross-device generalization and adversarial resilience.

REFERENCES

[1] D. D. Alves et al., "Authentication System Using Behavioral Biometrics Through Keystroke Dynamics," IEEE.
[2] J. Xiong and A. K. Belman, "Multi-Modal Adversarial Activity Detection Using Keyboard and Mouse Dynamics," IEEE.
[3] T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," ACM SIGKDD.
[4] C. Cortes and V. Vapnik, "Support-vector networks," Machine Learning.
[5] L. R. Rabiner, "A tutorial on hidden Markov models," Proc. IEEE.
[6] B. Li et al., "Wrist in Motion: Continuous Authentication Framework," IEEE TBIOM.
[7] J. Dybczak and P. Nawrocki, "Continuous Authentication on Mobile Devices," IEEE CCGrid.
[8] L. Szilágyi et al., "Mouse Dynamics for User Identity Authentication," IEEE LINDI.
[9] M. Killourhy and R. Maxion, "Anomaly Detection for Keystroke Dynamics," IEEE DSN.
[10] F. Monrose and A. Rubin, "Keystroke Dynamics as a Biometric," FGCS.
[11] S. Mondal and P. Bours, "Continuous Authentication Using Mouse Dynamics," IEEE TIFS.
[12] M. Mare et al., "ZEBRA: Bilateral Recurring Authentication," IEEE S&P.
[13] A. Buriro et al., "Smartphone Sensor-Based Behavioral Authentication," ICISC.
[14] H. Hu et al., "Adversarial Attacks Against Mouse Dynamics Authentication," ACM CCS.
[15] G. Shen et al., "Benchmark Study on Mouse Dynamics-Based Authentication," IEEE TIFS.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details