iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** III **Month of publication:** March 2026

DOI: https://doi.org/10.22214/ijraset.2026.77439

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

SENTRY: A Conceptual Review of Behavioral and Cognitive Biometric Authentication

Fatimatul Sharafa[1], Mashrifa[2], Gopika V[3], Agraj M[4], Ms Anagha M[5]
[1, 2, 3, 4]*Department of Computer Science and Engineering(CSE), Sree Narayana Guru College of Engineering and Technology Korom, Payyanur, Kannur*
[5]*Assistant Professor Department of Computer Science and Engineering (CSE), Sree Narayana Guru College of Engineering and Technology Korom, Payyanur, Kannur*

Abstract: Continuous user authentication is essential in modern digital systems to prevent session hijacking, identity misuse, and insider attacks. Conventional authentication mechanisms rely on one-time verification and fail to ensure security throughout an active session. To address this limitation, behavioral and cognitive biometrics offer a non-intrusive and adaptive approach to user authentication. This project presents a conceptual study of SENTRY, an adaptive behavioral– cognitive authentication framework designed for continuous user verification. The proposed system monitors user interaction patterns such as keystroke and mouse dynamics and integrates cognitive responses obtained through adaptive micro-challenges. Machine learning techniques are employed to model user behavior and detect anomalies, while a dynamic risk scoring mechanism enables real-time authentication decisions. The framework emphasizes usability, privacy awareness, and scalability, providing a robust foundation for secure and continuous authentication in modern computing environments.

I. INTRODUCTION

The growing dependence on digital systems has increased security risks such as identity theft, session hijacking, and insider attacks. Traditional authentication mechanisms, including passwords and one-time verification methods, fail to provide continuous protection after initial access is granted. As a result, unauthorized users may exploit active sessions without detection.

Behavioral biometrics offer a continuous authentication approach by analyzing user interaction patterns such as keystroke dynamics and mouse movements. However, behavioral patterns can vary due to environmental and cognitive factors, reducing reliability. To address this limitation, cognitive biometrics such as reaction time and error correction behavior can be incorporated. This work presents a conceptual study of SENTRY, an adaptive behavioral–cognitive authentication framework that combines continuous monitoring, adaptive micro- challenges, and risk-based decision-making to enhance security while maintaining usability.

II. RELATED WORK

Previous studies have proposed continuous authentication systems based on behavioral biometrics using machine learning techniques. While effective, these systems often suffer from behavioral drift and limited adaptability. Recent research integrates cognitive biometrics and risk-based authentication to improve reliability. However, few works present a unified framework that combines behavioral monitoring, cognitive assessment, adaptive micro- challenges, and real-time risk scoring. The proposed SENTRY framework addresses this gap by presenting a consolidated conceptual model for continuous user authentication.

III. LITERATURE REVIEW

1) Biometric Identification Based on Keystroke Dynamics

Kasprowski *et al.* [1] investigated biometric identification using keystroke dynamics by extracting timing-based features such as key press duration and inter-key latency. The study evaluated multiple classification techniques and demonstrated that keystroke dynamics can effectively distinguish users without requiring specialized hardware. The results confirmed the feasibility of behavioral biometrics for continuous authentication systems. The work highlights the advantages of keystroke-based identification in terms of cost efficiency, non-intrusiveness, and suitability for real-world deployment in security-sensitive applications.

2) User Attribution in Digital Forensics through Modeling Keystroke and Mouse Usage Data Using XGBoost

Gupta [2] proposed a user attribution framework for digital forensics using keystroke and mouse dynamics modeled with the XGBoost algorithm.

The study demonstrated that combining multiple behavioral features significantly improves attribution accuracy compared to single-feature approaches. The results emphasized the effectiveness of machine learning in identifying users based on interaction behavior. This work highlights the relevance of behavioral biometrics in forensic investigations and continuous authentication systems where accurate user identification is critical.

3) Free-Text Keystroke Dynamics for User Authentication

Li *et al.* [3] explored free-text keystroke dynamics as a method for continuous and unobtrusive user authentication. Unlike fixed-text approaches, the proposed method analyzed natural typing behavior during normal usage. The study demonstrated robust authentication performance in real-world scenarios and addressed practical challenges such as variability in typing patterns. The findings support the applicability of free-text keystroke dynamics for continuous authentication systems that require minimal user involvement and improved usability.

4) Distinguishability of Keystroke Dynamic Template

Sae-Bae and Memon [4] analyzed the distinguishability of keystroke dynamic templates by examining inter-user and intra-user variations. The study focused on the stability of behavioral features over time and evaluated their impact on authentication accuracy. The results highlighted challenges related to behavioral drift, feature consistency, and long- term reliability. This work provides valuable insights into the limitations of keystroke-based authentication systems and emphasizes the need for adaptive models in continuous authentication frameworks

5) A Generic Privacy-Preserving Protocol for Keystroke Dynamics-Based Continuous Authentication

Baig and Eskeland [5] proposed a privacy-preserving protocol for continuous authentication using keystroke dynamics. The study addressed key concerns related to biometric data leakage and user privacy by introducing secure data handling mechanisms. Experimental results showed that privacy protection can be achieved without significantly compromising authentication accuracy. This work is important for real-world deployment of behavioral biometric systems where data security, user trust, and compliance with privacy regulations are essential.

IV. CONCLUSION FROM LITERATURE REVIEW

The reviewed literature confirms that keystroke dynamics and behavioral biometrics are effective techniques for user identification and continuous authentication. Prior studies demonstrate that machine learning models can accurately analyze keystroke and mouse interaction patterns, enabling non-intrusive authentication without additional hardware. Research on free-text keystroke dynamics highlights improved usability and real-world applicability, while studies on template distinguishability reveal challenges related to behavioral drift and long-term stability. Privacy- preserving approaches further emphasize the importance of securing sensitive biometric data in continuous authentication systems. Although existing works address behavioral authentication from different perspectives, limited research integrates behavioral biometrics with cognitive assessment and adaptive risk-based decision mechanisms. The literature also lacks unified frameworks that combine usability, adaptability, and privacy within a continuous authentication model. These limitations motivate the proposed SENTRY framework, which aims to incorporate behavioral and cognitive features, adaptive micro-challenges, and dynamic risk scoring to enhance security and reliability in continuous user authentication systems.

V. PROPOSED SYSTEM ARCHITECTURE

The proposed system consists of three primary components:

A. Behavioral Data Capture Module

This module continuously monitors user interaction patterns such as keystroke dynamics, mouse movements, and touch inputs during normal system usage. The collected interaction data is preprocessed and relevant behavioral features are extracted in real time. This enables non- intrusive and continuous user monitoring without disrupting the user workflow.

B. Cognitive Assessment and Risk Scoring Engine

The cognitive engine introduces adaptive micro-challenges to evaluate cognitive response parameters such as reaction time, decision consistency, and error correction behavior. Machine learning models analyze both behavioral and cognitive features to compute a dynamic risk score. Based on predefined thresholds, the system determines the authentication confidence level and identifies potential anomalies.

C. Authentication Decision and Management Module

This module enforces authentication decisions based on the computed risk score. It manages access control actions such as allowing session continuation, triggering additional verification, or restricting access. An administrative interface supports system monitoring, user profile management, and audit logging, ensuring transparency and secure system operation.

VI. WORKING METHODOLOGY

The working methodology of the proposed SENTRY system is designed to provide continuous, adaptive, and secure user authentication while maintaining usability and privacy. The methodology follows a structured sequence of processes that enable real-time behavioral monitoring, cognitive assessment, and risk-based decision-making throughout an active user session.

A. User Interaction Data Acquisition

The process begins with continuous data acquisition during normal user activity. The system captures behavioral interaction data such as keystroke dynamics, mouse movements, and touch patterns. This data is collected passively without interrupting the user, ensuring that authentication remains non-intrusive and seamless.

B. Behavioral Feature Extraction

Once interaction data is captured, relevant behavioral features such as typing rhythm, inter-key latency, mouse movement speed, and click patterns are extracted. These features represent unique user behavior and form the basis for continuous identity verification.

C. Cognitive Assessment via Micro-Challenges

To enhance authentication reliability, the system introduces adaptive micro-challenges at appropriate intervals. These challenges evaluate cognitive parameters such as reaction time, decision consistency, and error correction behavior. The difficulty and frequency of challenges are dynamically adjusted based on observed user behavior.

D. Machine Learning-Based Analysis

Extracted behavioral and cognitive features are processed using machine learning models trained to learn individual user patterns. The models continuously compare real-time data with stored user profiles to detect deviations that may indicate unauthorized access.

E. Dynamic Risk Score Generation

Based on the deviation analysis, a dynamic risk score is computed to quantify authentication confidence. The risk score reflects the likelihood of user authenticity and adapts over time to behavioral drift, ensuring accurate decision- making.

F. Authentication Decision and Response

The computed risk score is evaluated against predefined thresholds to determine the appropriate system response. Low-risk sessions continue uninterrupted, while medium- risk scenarios trigger additional verification. High-risk conditions result in access restriction or session termination.

G. Auditability and Profile Adaptation

All authentication decisions and risk assessments are logged for auditability and system evaluation. Legitimate behavioral changes are gradually incorporated into the user profile, enabling adaptive learning while maintaining security.

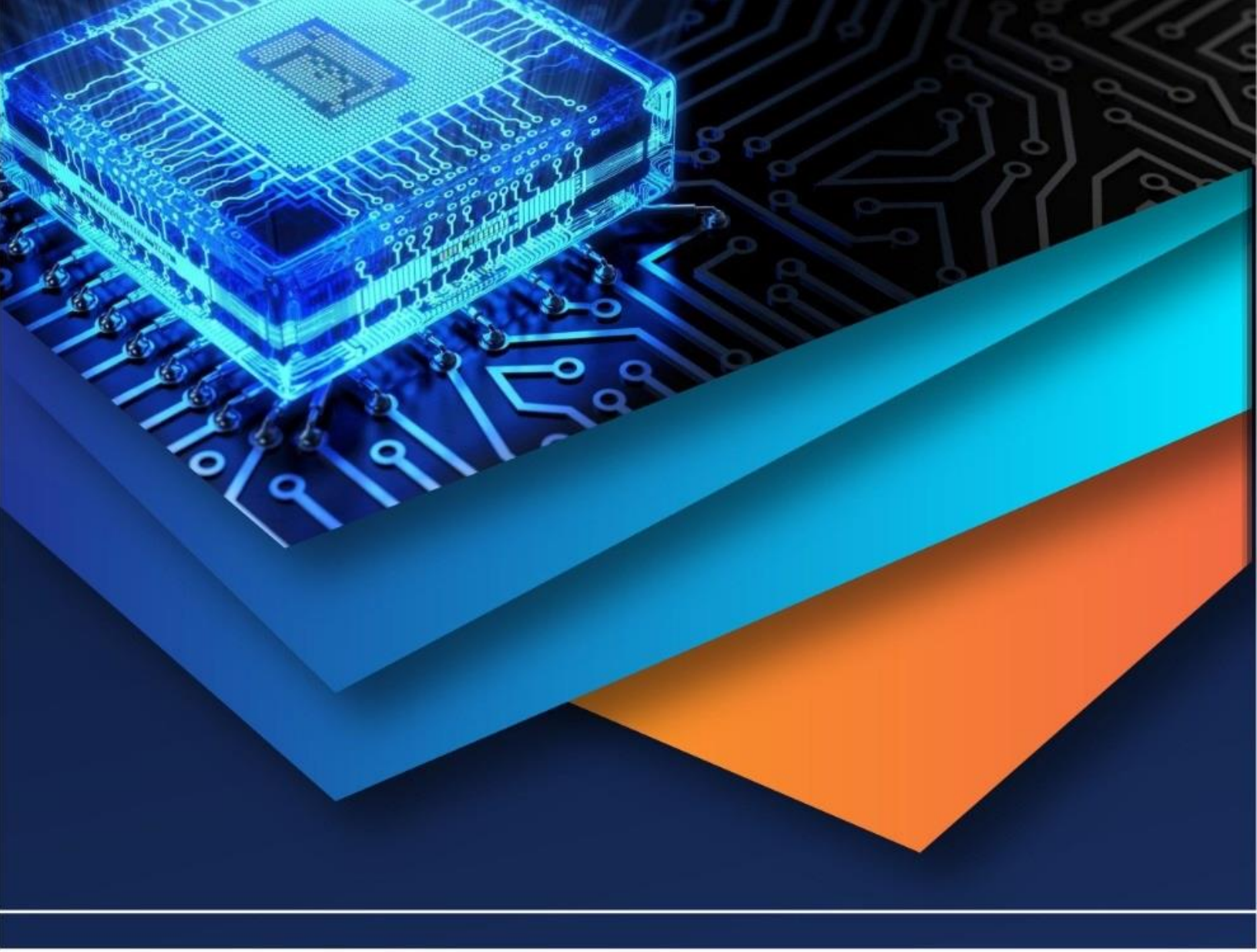
H. Summary of Methodology Significance

The proposed methodology demonstrates how behavioral biometrics, cognitive assessment, and machine learning can be combined to achieve continuous and adaptive authentication. By integrating micro-challenges and dynamic risk scoring, SENTRY provides a robust framework capable of detecting unauthorized access while preserving usability and privacy.

REFERENCES

[1] P. Kasprowski, Z. Borowska, and K. Harezlak, "Biometric Identification Based on Keystroke Dynamics," Sensors, vol. 22, no. 12, pp. 1–15, 2022.

[2] S. Gupta, "User Attribution in Digital Forensics through Modeling Keystroke and Mouse Usage Data Using XGBoost," International Journal of Computer Applications, vol. 184, no. 3, pp. 1–10, 2022.
[3] J. Li, H.-C. Chang, and M. Stamp, "Free-Text Keystroke Dynamics for User Authentication," IEEE Transactions on Information Forensics and Security, vol. 16, pp. 451–464, 2021.
[4] N. Sae-Bae and N. Memon, "Distinguishability of Keystroke Dynamic Template," IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 4, no. 1, pp. 28–40, 2022.
[5] A. F. Baig and S. Eskeland, "A Generic Privacy- Preserving Protocol for Keystroke Dynamics-Based Continuous Authentication," Computers & Security, vol. 115, pp. 102–123, 2022.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY