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

A survey on AI-Based Behavioral Biometrics for Continuous Identity Detection

[1]Futtaim Asim Khan, [2] Divya S Madhu Babu, [3]Abhinav Arya, [4] Ria Raviraj Urval,

[5] Dr. Mohammed Tajuddin

[1]Student, [2]Student, [3]Student, [4]Student, [5]Professor

[12345]Computer Science Engineering (Cyber Security),

[12345] Dayananda Sagar College of Engineering, Bangalore, India

Abstract : Behavioral biometrics provide a continuous and effortless way to verify user identity. Instead of depending only on passwords, these systems study how users type, move their mouse, or interact with a touchscreen. These everyday patterns are unique to each user and are hard for attackers to copy. In this paper, we explain how artificial intelligence models analyze these patterns to protect identity throughout a session. We combine keystroke dynamics, mouse movement behavior, gesture patterns, and machine learning models into one complete framework. Our findings show that models such as LSTM encoder–decoders and transformer networks can reach over 95% accuracy. Password similarity models like Pass2Path also help detect reused or slightly changed passwords with up to 67.51% success within 1000 guesses. Our framework helps identify account takeover attempts, insider misuse, and abnormal behavior while keeping user experience smooth and protecting privacy. We also explain how to deploy such systems in a hybrid client–server mode and how they perform in real scenarios.

IndexTerms - Behavioral Biometrics, Keystroke Dynamics, Continuous Authentication, Machine Learning, Identity Verification

I. Introduction

Passwords alone are no longer enough for secure authentication. Many attacks happen today because passwords are stolen, reused, or slightly modified across multiple platforms. By 2017, more than 5 billion passwords had leaked worldwide, and about 40% of users reused passwords [26], [27]. Once an attacker gets a password, they can use it until someone notices the breach [26]. Behavioral biometrics solve this problem by analyzing how a user interacts with a device. Typing rhythm, mouse speed, and gesture habits are unique to each person and very difficult to fake [12], [21]. When combined with AI, these patterns can be checked continuously throughout a session [5], [13]. This continuous checking supports the Zero Trust model, where every action must be verified [14], [15]. It also works in the background without asking the user to do extra steps. This paper reviews key research areas like keystroke dynamics [1], [3], mouse behavior [12], [21], gesture biometrics [2], [4], deep learning models [4], [5], and password similarity detection [7], [8]. We also discuss privacy protection [14], [16], deployment strategies [13], [17], [18], challenges, and future improvements [20], [26], [27].

II. Behavioral Biometrics and Keystroke Dynamics

A. Historical Background

The ”Fist of the Sender,” a tapping pattern used to identify Morse code operators, gave rise to keystroke dynamics during World War II [3]. This demonstrated early proof that people can be uniquely identified by their time patterns.

B. Typing-Based Timing Features

There are two main timing features used:

Dwell Time:

$$D_i = t_{release,i} - t_{press,i}$$

Flight Time:

$$F_i = t_{press,i+1} - t_{release,i}$$

Two users will still have different timing patterns even if they type at comparable speeds. Research indicates that utilizing models such as Random Forest and Deep Belief Networks, keystroke dynamics can provide 82–95% accuracy [1], [5], [6].

C. Mouse Dynamics and Other Behavioral Signals

There are other behaviors besides typing that aid in user identification. Additionally, mouse movement patterns provide helpful information. Among them are:

- moving speed
- accelerating and the smoothness
- clicking duration
- scrolling actions

Research indicates that each person has different mouse pathways, scrolling speeds, and click patterns [12], [21]. Authentication is strengthened when these patterns are used with data entry [12], [13], [21]. Touchscreen motions are another powerful biometric signal, especially on mobile devices.

Transformer-based models such as SwipeFormer perform remarkably well on swipe and gesture data. SwipeFormer succeeded:

- 6.6% EER on Android
- 3.6% EER on iOS

Compared to before feature based methods, this is better [4].

III. Continous Authentication

Instead than verifying the user's identity just once during login, continuous authentication verifies it continuously throughout the session. The system creates a baseline of typical behavior to do this [13], [14]. Examples of baselines include:

- Typical login times
- typical locations
- popular apps used
- file or menu opening behaviors
- typical mouse and typing patterns

The following machine learning techniques are employed for ongoing authentication:

- One-Class SVM
- Hidden Markov Models (HMMs)
- LSTM autoencoders

These machine learning models learn what is normal and flag unusual behavior as suspicious [5], [13].

Real-world systems show strong performance. For example, mobile banking apps using touch biometrics reached:

- static verification EER: 9.85%
- post-login EER: 1.88%
- continuous authentication F1 score: 94–97%

This shows that continuous authentication is practical and accurate [4], [13].

IV. Deep Learning For Behaviarol Biometrics

A. LSTM Models

LSTM networks work well for behavioral sequences because they can remember patterns over time [5]. In an LSTM autoencoder:

- the encoder compresses the behavior sequence
- the decoder tries to rebuild it

If the reconstructed output is very different from the original, the system detects an anomaly:

$$E = \| X - X\hat{} \|\, 2,\ E > \tau \Rightarrow \text{anomaly}$$

B. Transformer Models

Transformers use self-attention to study the entire sequence at once [4], [8]. The self-attention formula is:

$$\text{Attention}(Q, K, V) = \text{softmax}\,(QK^{T}/\sqrt{dk})V$$

V. Password Similarity and Credential Tweaking Detection

Many users change their passwords slightly or reuse them, such as:

- Including numbers (password → password1)
- Including a year (password → password2024)
- Making the initial letter capital

These patterns are used by attackers to guess passwords [26], [27]. Pass2Path discovers how users change their passwords. Changes are modeled as edit steps:

$$ei = (ti\ ,\ ci\ ,\ \ell i)$$

Pass2Path achieved:

- 48% of password guesses are successful after 1000 attempts (simulation)
- 8.4% of authentic university accounts are cracked [7]

PassTrans improved this to:

67.51% success within 1000 guesses

Password similarity analysis is essential for preventing account takeover attempts [8], [26].

VI. User and Entity Behavior Analytics (UEBA)

UEBA systems keep an eye on device and user behavior to identify:
• suspicious activity
• compromised accounts
• insider threats
• credential abuse Industry reports state that:
• According to 64% of cybersecurity professionals, insiders are the biggest threat.
• UEBA tools are used by just 44% of firms.
UEBA uses anomaly detection, clustering, PCA, and supervised models. [9]–[11].
These improve the identification of compromised sessions, policy violations, and insider misuse. [24], [25].

VII. Technical Architecture and Methodology

A. Behavioral Data Collection

A thorough behavioral biometric system gathers all kinds of user behavior. [12], [14], [17]. These include:
• Keystroke timing: dwell time, flight time and time of the day
• Mouse movements: speed, accelerating and the smoothness
• Touch gestures: gesture shape, pressure, and swipe speed
• Device usage patterns: file access, menu navigation, and programs utilized
One way to express a feature vector is as:

$$xi = [t1, t2, \ldots, d1, d2, \ldots, s1, s2, \ldots] \top$$

B. Feature Engineering

It is necessary to transform raw data into meaningful features [1], [5]. Typical characteristics consist of:
• Timing ranges, variance, and averages
• Trigraph and digraph sequences
• normalized rhythmic elements
• Contextual elements such as the time of day or the use of applications
Additionally, deep learning models are capable of autonomously extracting characteristics. [4], [5].

C. Anomaly Detection Algorithms

LSTM Autoencoder:

$$E = \| X - X\hat{} \| 2$$

Abnormal behavior is indicated by large errors. [5].
One Class SVM: Indicates that a behavior is abnormal if

$$f(x) < 0$$

A common technique for identifying anomalies in behavioral analysis [13].
Markov models that are hidden (HMMs): Unusual behavior is indicated by low sequence likelihood. [5], [13].

D. Risk Scoring

One score is created by combining many anomalous signals:

$$R = \sum_{i=0}^{n} w_i s_i$$

UEBA and continuous authentication systems make extensive use of risk rating frameworks. [9], [24], [25].

VIII. Detection Performance

A. Keystroke Dynamics

High accuracy is attained by keystroke models:
• Random Forest: 93% accuracy [1]
• DBN: 95% accuracy [6]
• LSTM autoencoder: 92% [5]
B. Touch Dynamics
Mobile authentication systems reached:
• 9.85% EER (static)
• 1.88% EER (post-login)
• F1 score 94–97%
Recorded in ongoing assessments of authenticity [5], [13].
C. Gesture Recognition
SwipeFormer's transformer model reached:
• 6.6% EER on Android
• 3.6% EER on iOS [4]
D. Password Variant Detection
Password similarity models' outcomes:
• Pass2Path: 48% success in 1000 guesses [7]
• PassTrans: 67.51% of 1000 guesses were successful. [8]
These highlight the significance of modeling passwordediting patterns. [26], [27].

IX. Insider Threat and Account Takeover Detection

A. Detecting Insider Threats:

These underline how important it is for simulating password-editing patterns.

Careless insiders: Urgent modifications point to accounts being compromised. [9], [10].

Insiders with malicious intent: Unusual file access or activity during off-peak hours [10], [25].

Insiders who were compromised: Mouse and typing habits don't reflect the actual user. [12], [21].

B. Account Takeover Defense:

Anomalies include:

• logins from places where travel is not possible

• strange file navigation or menu

• discrepancy in typing style

Even after login, behavioral biometrics improve identification verification. [13], [17], [18].

X. Privacy and Security Considerations

A. Privacy Protection

To keep behavioral data safe:

• use behavioral hashing

• store only the features that are really needed

• follow the CCPA and the GDPR requirements [14], [16], [18]

Corporate deployments require authentication that protects privacy. [17], [18].

B. Spoofing Resistance

Behavior is really difficult to fake because:

• Users behave unintentionally

• Long sessions cannot be imitated by adversaries.

• Fakes are exposed by minute timing variations.

Strong spoof-resistance across behavioral modalities is confirmed by studies. [12], [20], [21].

XI. Integration with Enterprise Systems

A. Deployment Models

Three deployment approaches:

Client-side: Quick, private, and offline [17].

Server-side: More processing power and large models [14], [18].

A hybrid: Quick local tests and more thorough server checks [18].

B. SIEM/SOC Integration

SIEM systems such as Splunk, Microsoft Defender, or Exabeam can receive behavioral warnings to integrate with:

• logs of access

• abnormalities in the network

• Abuse of privilege

SIEM-driven correlation improves the quality of detection [24], [25].

XII. Research Challenges and Future Work

A. Behavioral Drift

Over time, user behavior shifts. Models need to adjust without overlooking attacks. [20].

B. Environmental Variability

Different gadgets (phone, tablet, laptop) have an impact on behavior. [14], [16].

C. Cross-Platform Consistency

Many different systems are used by organizations. Behavior models need to be applicable to all [17], [18].

D. Adversarial ML Attacks

Attackers may attempt to trick models by making minor adjustments. Adversarial training, ensembles, and anomaly filters are examples of defenses. [26], [27].

XIII. Conclusion

Artificial intelligence-enhanced behavioral biometrics offer a significant breakthrough in ongoing identification verification. These systems continuously track keystrokes, mouse movements, touchscreen gestures, and password modification habits to create multifaceted behavioral profiles, in contrast to traditional authentication, which verifies individuals only at login [12], [14], [16]. LSTM autoencoders, transformers, and ensemble architectures are examples of machine learning models that may identify behavioral abnormalities with accuracy higher than 95% [4], [5], showing great promise for preventing fraud, safeguarding accounts, and providing safe user experiences in business and financial settings.

The identification of insider attacks, account takeovers, and advanced persistent threats is strengthened by integrating behavioral analytics with UEBA, SIEM, and IAM platforms [9], [24], [25]. By correlating behavioral signals with conventional security logs, these integrations allow enterprises to swiftly and precisely identify anomalous access patterns, privilege misuse, and high-risk actions [10], [11]. By examining frequent user patterns to reuse or slightly alter passwords, password similarity models like Pass2Edit and PassTrans further aid in the early detection of credential tweaking attempts [7], [8], [26]. These features stop hackers from taking advantage of predictable password-editing habits, which frequently result in account penetration [27].

Continuous behavioral authentication does not compromise user privacy thanks to privacy-preserving strategies like behavioral hashing, stringent data minimization, and adherence to legal frameworks like the CCPA and GDPR [14], [16], [18]. To balance model accuracy and user confidentiality, modern authentication platforms are increasingly using encrypted computing techniques,

hybrid client-server models, secure ondevice processing, and anonymized feature representation [13], [17]. These advancements support the reliability of behavioral systems in delicate settings including government services, banking, and healthcare.

As behavioral systems grow in size, a number of obstacles still exist. Adapting to natural changes in user behavior, maintaining consistency across different devices, standardizing feature extraction for multi-device usage, and thwarting malicious manipulation are important concerns [20], [26], [27]. Adaptive and robust models are necessary to maintain high accuracy in the face of variations brought on by environmental noise, hardware variations, posture changes, stress levels, and long-term behavioral drift. Furthermore, since cybercriminals are experimenting more and more with adversarial inputs and mimicking tactics, future research must prioritize developing strong security mechanisms [20].

Continuous model retraining, adaptive learning techniques, multimodal fusion of behavioral signals, and enhanced spoofdetection algorithms must all be investigated in future research [15], [18]. Stronger and more resilient identity assurance could be achieved by combining keystroke dynamics, mouse analytics, touchscreen biometrics, geolocation behavior, and device usage patterns. For businesses managing millions of active sessions at once, research on scalable cloud-native architectures, decentralized identity systems, zero-trust integration, and real-time decision engines will also be crucial. The need for AI-driven behavioral identity systems will only increase as digital ecosystems evolve.

In general, proactive, ongoing identity assurance replaces reactive credential validation as a result of the convergence of AI and behavioral biometrics. These technologies have the ability to completely transform safe access across contemporary digital platforms, financial services, and international high-risk infrastructures by combining intelligent behavioral models, strong anomaly detection, privacy-preserving computation, and enterprise-grade threat analytics. Behavioral biometrics are positioned as a crucial cornerstone for the upcoming generation of cybersecurity due to its capacity to offer seamless, frictionless, and persistent identity protection.

ACKNOWLEDGEMENT

The authors would like to express their gratitude to Dr. Mohammed Tajuddin of the Department of Computer Science and Engineering (Cybersecurity), Dayananda Sagar College of Engineering, for his excellent advice, constant encouragement, and mentorship during this research project.

REFERENCES

[1] Detection of Facial Micro Expressions and Textual-Tracking for Paralyzed Using Computer Vision, International Journal of Computer Sciences and Engineering, Vol.7, Issue 12, pp.62–66, 2019. Available: https://doi.org/10.26438/ijcse/v7i12.6266

[2] Cryptographic Key Generation using Retina Biometric, IJEIT Journal. Available: https://d1wqtxts1xzle7.cloudfront.net/83014536/ IJEIT1412201307 10-libre.pdf

[3] A. Sharma, M. Jurec˘ek, and M. Stamp, "Keystroke dynamics for user identification," arXiv preprint arXiv:2307.05529, 2023.

[4] P. Delgado-Santos et al., "SwipeFormer: Transformers for mobile touchscreen biometric verification," Expert Systems with Applications, vol. 237, p. 121537, 2024.

[5] S. Oduri, "Continuous authentication and behavioral biometrics: Enhancing cybersecurity in the digital era," IJIRSET, vol. 13, no. 7, 2024.

[6] A. O. Aljahdali, "Dynamic keystroke technique for a secure authentication system based on deep belief nets," Engineering, Technology & Applied Science Research, vol. 13, no. 3, 2023.

[7] D. Wang et al., "PASS2EDIT: A multi-step generative model for guessing edited passwords," in Proc. USENIX Security Symposium, 2023.

[8] X. He et al., "PassTrans: An improved password reuse model based on Transformer," IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 3, 2023.

[9] Exabeam, "UEBA (User and Entity Behavior Analytics): Complete 2025 guide," 2025. Available: https://www.exabeam.com/explainers/ueba/

[10] Varonis, "What is UEBA? Complete guide to user and entity behavior analytics," Nov. 2024. Available: https://www.varonis.com/blog/ user-entity-behavior-analytics-ueba

[11] CrowdStrike, "What is User and Entity Behavior Analytics (UEBA)?" Sept. 2025. Available: https://www.crowdstrike.com/ en-us/cybersecurity-101/identity-protection

[12] TypingDNA, "What is mouse dynamics and how it works," Dec. 2024. Available: https://www.typingdna.com/glossary/ what-is-mouse-dynamics

[13] 1Kosmos, "Continuous authentication: A dynamic approach to user verification," Mar. 2025. Available: https://www.1kosmos.com/ authentication/continuous-authentication-guide

[14] IBM, "What is behavioral biometrics?" June 2025. Available: https:// www.ibm.com/think/topics/behavioral-biometrics

[15] Citrix, "What is continuous authentication?" Nov. 2024. Available: https: //www.citrix.com/glossary/what-is-continuous-**authentication.html**

[16] LexisNexis Risk Solutions, "What is behavioral biometrics," Oct. 2025. Available: https://risk.lexisnexis.com/global

[17] Celebrus, "Behavioral biometrics for continuous authentication," Dec. 2024. Available: https://www.celebrus.com

[18] Akitra, "Continuous authentication with behavioral biometrics," June 2024. Available: https://akitra.com/blog

[19] MojoAuth, "Behavioral authentication anomaly detection," July 2025. Available: https://mojoauth.com

[20] Securitum, "Challenges of behavioral biometrics security," Nov. 2023. Available: https://www.securitum.com

[21] Plurilock, "Deep dive: Mouse dynamics," Feb. 2024. Available: https: //plurilock.com

[22] AuthGear, "How behavioral biometrics are changing authentication," Oct. 2025. Available: https://www.authgear.com

[23] Z. Luo, J. Liu, and S. Zhu, "MDP-AD: An adaptive framework for vulnerability detection," Journal of Computer Security, vol. 33, 2025.

[24] Splunk, "User behavior analytics solutions," Dec. 2024. Available: https: //www.splunk.com

[25] Fortinet, "What is User Entity and Behavior Analytics (UEBA)?" Dec. 2024. Available: https://www.fortinet.com

[26] SSH.com Academy, "Types of password attacks and prevention strategies," Feb. 2025. Available: https://www.ssh.com

[27] Software Secured, "Top 10 credential based attacks," Oct. 2025. Available: https://www.softwaresecured.com