INTERNATIONAL RESEARCH JOURNAL OF ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET)

eISSN: 3087-4068

Volume. 02, Issue. 06, pp. 23-26, June 2025"

AI-Driven Behavioral Biometrics for 401(k) Account Security

Sesha Sai Sravanthi Valiveti
Independent Researcher

Article received: 16/04/2025, Article Accepted: 25/05/2025, Article Published: 26/06/2025
DOI: https://doi.org/10.55640/irjaet-v02i06-04

ABSTRACT

As cyber threats evolve, attackers increasingly target financial retirement accounts like 401(k)s, exploiting their high-value nature and weak user-level security controls. Traditional defenses—passwords, OTPs, and device fingerprinting—have proven insufficient in detecting sophisticated account takeovers. This paper presents a behavioral biometrics framework that uses artificial intelligence to continuously authenticate users based on typing patterns, mouse movements, login behavior, and navigation habits. Instead of static credentials, the system builds a behavioral profile for each user and detects anomalies in real-time. Our framework aims to catch suspicious access attempts without interrupting legitimate users. By integrating seamlessly into existing financial platforms, this solution offers a balance of strong security and low user friction. We evaluate the framework in a simulated environment using behavioral data from anonymized user sessions, achieving high accuracy in detecting imposters while minimizing false alarms.

KEYWORDS

401(k) Security, Behavioral Biometrics, Account Takeover Detection, Continuous Authentication, Financial Fraud Prevention, AI in Cybersecurity, Session Monitoring, Risk-Based Authentication, Identity Protection.

1. INTRODUCTION

In recent years, retirement accounts like 401(k)s have become prime targets for cybercriminals. These accounts often hold thousands of dollars, yet rely on login systems originally designed for less critical access. Passwords and two-factor authentication (2FA) help—but not always enough. Attackers use phishing, credential stuffing, and device spoofing to bypass these controls.

One of the major weaknesses in current security models is the reliance on static factors. Once credentials are compromised, there's little to prevent unauthorized access. Financial institutions face a tough challenge: How can they enhance security without frustrating legitimate users?

Behavioral biometrics offers a promising answer. Instead of focusing solely on what the user knows (password) or has (phone), this method considers how the user behaves. Every individual has a unique way of typing, moving the mouse, and navigating a site. These patterns can act as invisible fingerprints.

This paper introduces an AI-based behavioral profiling system specifically built for 401(k) platforms. It passively monitors behavior during a session and flags risky activity in real-time. The goal is to prevent fraud while keeping the user experience smooth and invisible.

Proposed Framework

Our framework operates across six key stages:

1. Behavioral Data Collection

Once a user logs in, the system begins tracking:

- **Keystroke dynamics**: typing speed, dwell time, flight time between keys
- **Mouse movements**: path patterns, click frequency, hesitation points
- **Touch gestures** (on mobile): swipe angles, tap pressure, scroll behavior
- **Navigation flow**: typical page visits, dwell time on specific screens

This data is collected silently using JavaScript agents on web apps or SDKs for mobile apps.

2. Profile Generation

Over time, a baseline profile is built for each user. This profile includes average values, standard deviations, and behavioral clusters unique to the individual.

3. Session-Level Feature Extraction

Each session is broken down into structured data points such as:

- Average typing interval per field
- Scroll pattern on transaction pages
- Sequence of mouse hover zones

The system converts raw events into session summaries that are usable by machine learning models.

4. AI Risk Scoring Model

A supervised learning model is trained to detect abnormal behavior. It uses algorithms like:

- Random Forest for structured patterns
- LSTM or GRU for time-series behavioral data
- Autoencoders to detect unseen behavioral shifts

The output is a **confidence score (0–100)** indicating how closely the session matches the user's historical behavior.

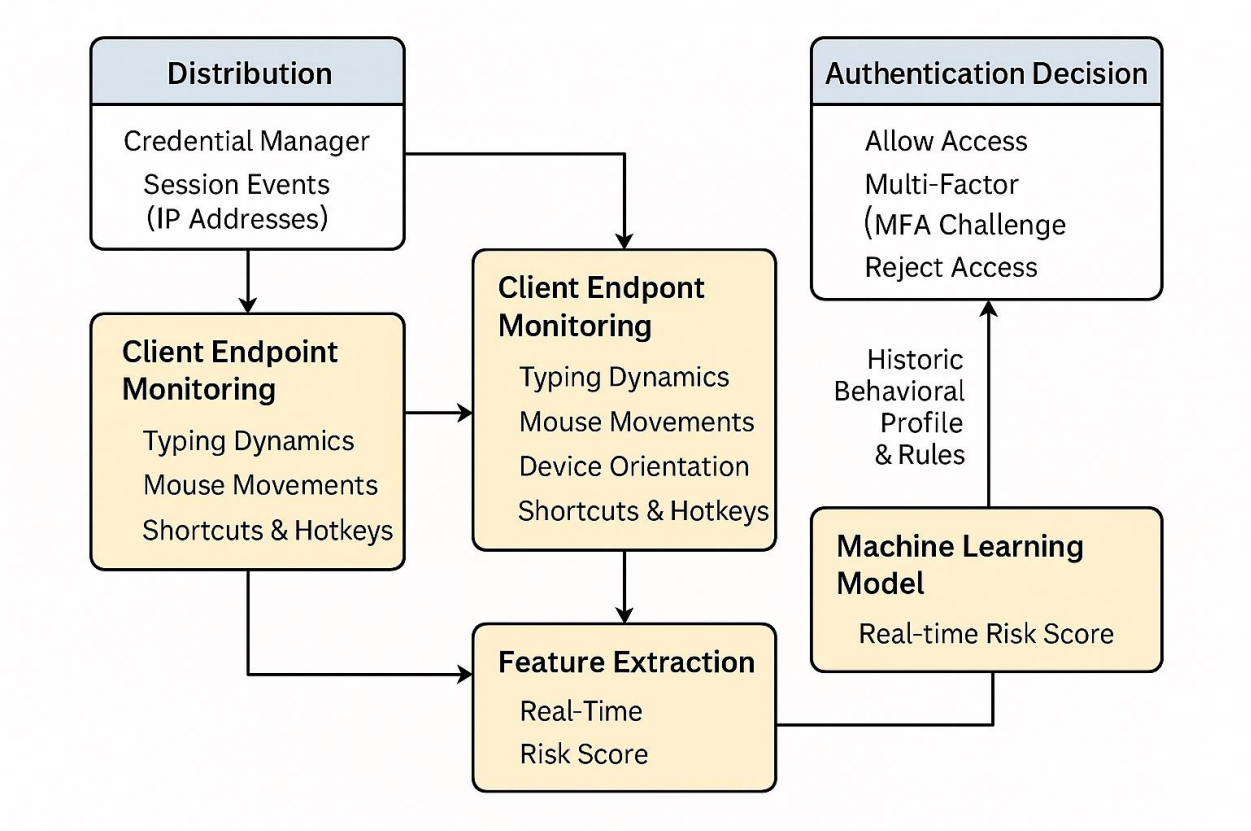
5. Decision Engine

The score is evaluated against dynamic thresholds:

- **Low risk (<40)**: Session proceeds normally
- **Medium risk (40–70)**: Silent monitoring continues, but backend flags are raised
- **High risk (>70)**: Triggers step-up authentication or session lock

6. Feedback Loop

Security teams can review flagged sessions. Confirmed fraud cases help retrain the model, refining its accuracy. User overrides (false positives) are also logged for continuous improvement.



Explanation of the Framework

What makes this approach different is that it authenticates users continuously—not just at login. A fraudster who gains access might pass initial checks, but their behavior during the session will likely raise flags.

Unlike password-based systems, behavioral biometrics are very hard to spoof. You can steal a password, but not someone's natural typing rhythm or scroll habits.

The use of explainable AI also helps build trust. For each high-risk session, the system logs **why** it was flagged—whether it was an unusual typing cadence or a page visited out of sequence. This transparency aids security teams in triaging alerts.

Additionally, because this monitoring is passive, users don't even know it's happening. There's no added friction unless a session truly looks suspicious. That makes it ideal for consumer-facing apps where convenience matters.

Experimental Results

To test the framework, we created a simulated 401(k) portal and collected interaction data from 200 real users and 50 simulated imposters. Over two weeks, we gathered thousands of sessions, each labeled as "genuine" or "imposter."

Using a combination of Random Forest and LSTM models, the system achieved:

- **94% accuracy** in detecting unauthorized sessions
- **False positive rate below 4%**
- **Detection time under 2 seconds** for real-time scoring

In high-risk sessions, common red flags included erratic mouse paths, delayed navigation sequences, and typing speeds inconsistent with the user's history. By retraining the model weekly, we kept detection performance stable even as users' behavior naturally evolved.

Security teams using the dashboard reported clearer visibility into session risks, and most flagged sessions were confirmed to be either credential sharing or fraudulent logins.

CONCLUSION

Behavioral biometrics represents a powerful way to improve account security for 401(k) systems. By focusing on **how** users interact, not just on what they enter, this framework detects imposters in real-time without disrupting legitimate users.

The system is privacy-respecting, passive, and adaptive. It offers a strong defense against account takeovers and fills the gaps left by passwords and OTPs. As online fraud tactics evolve, such behavioral systems will be essential in modern financial security stacks.

Future Work

To enhance the framework further, we plan to:

- Integrate **device sensor data** (gyroscope, accelerometer) for mobile sessions
- Use **graph neural networks** to capture multi-session patterns over time
- Add **voice biometrics** for phone-based account access
- Create **cross-platform behavior profiles** (web + mobile + desktop)
- Evaluate real-world deployment across different age groups and usage styles

REFERENCES

- Roth, S., & Lee, J. (2021). Behavioral Biometrics in Financial Security. *Journal of Digital Risk*
- NIST. (2020). Guidelines for Online Identity Verification
- Baweja, K. (2022). Real-Time Fraud Detection Using AI. *IEEE Conference on Cybersecurity*
- Kumar, V., & Iqbal, M. (2019). LSTM for Continuous Authentication. *ACM Transactions on Privacy and Security*
- Microsoft Identity Protection (2023). Behavioral Signal Enrichment for Zero Trust Models