ISSN: 2755-6190

Research Article

Open Access Journal of Artificial Intelligence and Technology

Presenting an Operational Model for Adaptive Biometric Authentication with multi-feature Combination

Mohammad Taleghani[1*] and Fatemeh Alidoosti Hesari[2]

[1]*Department of Industrial Management, Ra.C., Islamic Azad University (IAU), Rasht, Iran*
[2]*Department of Industrial Engineering, Te.C., Islamic Azad University(IAU), Tehran, Iran*

[*]**Corresponding author**
Mohammad Taleghani, Department of Industrial Management, Ra.C., Islamic Azad University (IAU), Rasht, Iran.

Received: December 19, 2025; **Accepted:** December 23, 2025; **Published:** December 29, 2025

ABSTRACT

Adaptive biometric authentication is increasingly viewed as a cornerstone of secure digital interaction in environments characterized by escalating attack sophistication and the growing use of synthetic identities. This study proposes and analytically substantiates a practical implementation model of adaptive biometric authentication based on multi-feature fusion of physical and behavioral biometric traits. The core premise of the work is that static biometrics alone no longer provide sufficient resilience against replay attacks, spoofing, and data leakage, while behavioral signals in isolation suffer from instability and context sensitivity. The proposed model integrates fingerprint and facial features with keystroke dynamics and mouse movement patterns into a unified trust-scoring framework governed by a self-adaptive machine learning engine. A hybrid architecture is examined in which heterogeneous biometric streams are synchronized, normalized, and fused at the decision level to produce a composite authentication score that evolves over time. The study employs experimental validation on a multimodal dataset that simulates realistic access scenarios under both legitimate and adversarial conditions. Quantitative evaluation demonstrates that adaptive multi-feature fusion achieves a statistically significant reduction in false acceptance rates while preserving usability under natural behavioral drift. Special attention is given to the role of real-time model updating and continuous authentication, which together form the operational core of a patented multi-level biometric authentication system used as a reference implementation.

Keywords: Adaptive Authentication, Biometric Fusion, Behavioral Biometrics, Keystroke Dynamics, Trust Score Modeling, Machine Learning in Cybersecurity, Continuous Authentication, Multi-Level Biometric Systems.

Introduction

Biometric authentication has evolved from a specialized security mechanism into a foundational component of contemporary digital identity management. The rapid expansion of remote access services, cloud infrastructures, mobile platforms, and critical digital services has transformed authentication from a peripheral control function into a central pillar of cybersecurity architectures. Traditional password-based schemes are now widely recognized as inadequate due to their inherent vulnerability to phishing, credential reuse, social engineering, and large-scale database breaches [1,2]. In response, biometric technologies based on physiological traits such as fingerprints, facial geometry, and iris patterns have been widely adopted as stronger substitutes for knowledge-based credentials. However, the increasing availability of high-fidelity biometric sensors, deepfake generation tools, and spoofing kits has fundamentally altered the threat landscape, exposing even advanced physical biometrics to replay and presentation attacks [3-5].

Problem Statement

Parallel to the maturation of physical biometrics, behavioral biometrics has emerged as a complementary authentication paradigm grounded in the unique dynamic patterns of human interaction with digital systems. Keystroke dynamics, mouse trajectories, touch gestures, and temporal interaction rhythms offer continuous, context aware signals that are difficult to replicate with precision and can be monitored throughout an

Citation: Mohammad Taleghani, Fatemeh Alidoosti Hesari. Presenting an Operational Model for Adaptive Biometric Authentication with multi-feature Combination. Open Access J Artif Intel Tech. 2025. 1(2): 1-5. DOI: doi.org/10.61440/OAJAIT.2025.v1.16

active session [6-8]. Despite their conceptual advantages, behavioral features exhibit pronounced intra-user variability driven by fatigue, emotional state, device heterogeneity, and environmental context. This instability limits their reliability when applied as standalone authentication factors in high assurance systems.

The current generation of secure access platforms therefore increasingly relies on multimodal biometric integration, where physical and behavioral traits are jointly analyzed to reduce uncertainty and improve robustness.

Yet, the majority of deployed systems still implement such integration in a predominantly static or rule-based manner, applying fixed thresholds and manually tuned weight coefficients that fail to adapt to long term behavioral drift or evolving attack strategies [9.10]. As a result, these systems demonstrate degraded performance over extended operational lifecycles and remain vulnerable to targeted adversarial manipulation. Adaptive biometric authentication seeks to overcome these limitations by embedding machine learning directly into the biometric decision pipeline. In adaptive frameworks, biometric reference models evolve continuously based on verified user behavior, and trust scores are recalibrated in real time to reflect both short term anomalies and long-term profile changes [11,12]. This paradigm aligns naturally with zero-trust security architectures, where access decisions are treated as dynamic risk assessments rather than static binary checks. Nevertheless, despite extensive theoretical exploration of adaptive fusion models, relatively few studies provide detailed, practically implementable system architectures that integrate heterogeneous biometric streams, risk scoring, and continuous learning into a unified operational platform.

Theoretical Gap Analysis

The present study addresses this gap by proposing and validating a practical implementation model of adaptive biometric authentication based on multi-feature fusion. The model combines two classes of biometric evidence. The first class comprises static physical biometrics, represented by fingerprint and facial recognition features. The second class consists of dynamic behavioral biometrics, including keystroke dynamics and mouse movement patterns captured during normal human computer interaction. These heterogeneous signals are processed through a unified analytical pipeline that performs feature normalization, probabilistic scoring, and decision-level fusion within a continuously adaptive machine learning framework. The resulting composite trust score serves as the primary decision variable governing access control and step-up authentication mechanisms. A distinctive feature of the proposed model lies in its grounding in a concrete patented system for multi-level biometric authentication with dynamic behavioral analysis. This reference implementation formalizes the architectural separation of physical and behavioral acquisition modules, introduces a dedicated artificial intelligence engine for composite trust computation, and incorporates reinforcement learning for continuous profile adaptation. Unlike many conceptual models described in the literature, the patented architecture explicitly supports real-time risk scoring, anomaly detection, and automated model updating under operational conditions. By anchoring the analytical framework of this study to a legally protected technical solution, the research bridges the persistent divide between theoretical biometric fusion research and deployable cybersecurity systems.

Research Methodology

The proposed adaptive biometric authentication model is grounded in a multi-level architecture that integrates physical and behavioral biometric evidence within a unified analytical and decision-making framework. The methodological foundation of this study combines system level architectural modeling, probabilistic trust score formulation, and adaptive machine learning for continuous profile updating. The practical feasibility of the model is validated through its correspondence with a patented multi-level biometric authentication system that implements real-time behavioral analysis and composite risk scoring. The authentication platform is structured as a sequence of tightly coupled processing modules. At the front end, an input module acquires heterogeneous biometric signals. Physical biometric data include fingerprint impressions captured through capacitive or optical scanners and facial images collected via RGB or infrared cameras. Behavioral biometric data are collected concurrently during user interaction, including keystroke timing vectors and cursor movement trajectories. These dual streams are processed in parallel and converge within a centralized artificial intelligence engine responsible for feature analysis and trust computation.

The architectural layout corresponds to a three-stage pipeline. The first stage performs synchronized acquisition and preprocessing of biometric signals. The second stage executes feature extraction and behavioral profiling in real time. The final stage is a decision module that fuses probabilistic outputs from the physical and behavioral classifiers to produce an access decision. This configuration mirrors the block-level architecture of the patented system, where independent physical and behavioral acquisition modules feed a common AI-driven decision core, followed by an outcome module responsible for access control enforcement and alert generation. Physical biometric features are represented using conventional template-based descriptors. For fingerprints, minutiae point distributions and ridge orientation histograms are used as the primary feature vectors. For facial recognition, deep convolutional embeddings extracted from a pretrained face recognition network serve as identity descriptors. These embeddings are normalized to unit length to stabilize similarity estimation across acquisition sessions.

Behavioral biometric features are modeled as multivariate time series. Keystroke dynamics are represented through inter-key latency, key hold duration, and digraph timing distributions. Mouse movement patterns are encoded using velocity, acceleration, curvature, and dwell-time heatmaps. These signals are sampled at fixed temporal resolution and segmented into interaction windows of uniform length. Each segment is transformed into a statistical feature vector that captures both short-term variability and session-level behavioral tendencies.

To ensure compatibility between heterogeneous feature spaces, all biometric features are subjected to z-score normalization using rolling statistics computed over the most recent verified sessions. This adaptive normalization enables the system to track slow behavioral drift while preserving sensitivity to abrupt deviations.The behavioral analysis engine is implemented as

a multilayer neural architecture comprising an input layer that ingests normalized feature vectors, multiple hidden layers for nonlinear feature interaction modeling, and an output layer that estimates the likelihood of legitimate user behavior. This layered structure corresponds directly to the reference machine learning model used for authentication decision-making in the patented system.

Model parameters are updated via online reinforcement learning. After each verified successful authentication, the behavioral reference profile is incrementally adjusted using stochastic gradient updates that minimize prediction error under confirmed legitimate input. In contrast, failed authentication attempts are used to update adversarial class boundaries and enhance anomaly sensitivity. This dual-update strategy ensures that the system remains responsive to gradual behavioral evolution without compromising its ability to detect abrupt fraudulent patterns.To mitigate catastrophic forgetting, a bounded historical memory buffer is maintained, retaining a sliding window of past legitimate feature distributions. Periodic rebalancing of model weights using this buffer stabilizes long-term behavior modeling under nonstationary interaction conditions.

Results

The experimental evaluation of the adaptive biometric authentication model was conducted under controlled yet operationally realistic conditions in order to assess both instantaneous classification performance and long-term stability under behavioral drift. The results demonstrate that adaptive multi-feature fusion significantly outperforms unimodal and static multimodal baselines across all principal security metrics. The analysis further confirms that continuous profile updating and dynamic trust score calibration is essential for maintaining robustness under nonstationary user behavior. Initial performance was assessed by comparing four authentication configurations: standalone physical biometrics, standalone behavioral biometrics, static multimodal fusion with fixed weights, and the proposed adaptive multimodal fusion model. Physical biometrics achieved high instantaneous accuracy under clean acquisition conditions but exhibited notable vulnerability to replay attacks and synthetic spoofing. Behavioral biometrics demonstrated superior resistance to direct replay but suffered from elevated false rejection rates due to natural intra-user variability.

Static multimodal fusion improved overall performance by combining both modalities, yet its fixed weighting scheme proved suboptimal under changing interaction dynamics. The adaptive fusion model consistently achieved the lowest equal error rate across all test sessions. On average, the adaptive system reduced the false acceptance rate by approximately 38 percent relative to static fusion and by more than 60 percent relative to unimodal physical authentication. At the same time, the false rejection rate remained within a narrow margin of operational usability even under varying environmental and device conditions. A critical dimension of performance concerned the system's ability to preserve authentication accuracy over time as legitimate user behavior evolved. Participants were observed over multiple sessions spanning several weeks. Non-adaptive behavioral models exhibited a gradual degradation in classification accuracy, with false rejection rates increasing steadily as typing rhythms and cursor control patterns shifted due to fatigue, changing devices, and contextual factors.

In contrast, the adaptive model maintained stable error rates throughout the observation period. The reinforcement learning based profile updating mechanism continuously realigned internal reference distributions with newly verified behavioral samples. As a result, the composite trust score distribution for legitimate users remained statistically stationary, while the distribution for impostor attempts remained clearly separated. This confirms that the adaptive learning loop embedded in the patented multi-level architecture effectively mitigates the long-term instability traditionally associated with behavioral biometrics.

Resistance to Spoofing and Imitation Attacks

Simulated attack scenarios included physical biometric replay, synthetic fingerprint and facial spoofing, and behavioral imitation based on recorded keystroke and mouse traces. Unimodal physical authentication exhibited the highest vulnerability to high-quality replay attacks, particularly for facial recognition under favorable lighting. Unimodal behavioral authentication resisted direct replay more effectively but showed partial susceptibility to skilled imitation over extended observation windows. The adaptive multimodal fusion model demonstrated the strongest resistance to all tested attack classes. In replay scenarios, the behavioral channel introduced high anomaly scores that suppressed the composite trust value below the acceptance threshold even when physical spoofing succeeded. In imitation scenarios, physical biometrics provided a stabilizing anchor that prevented behavioral mimicry from achieving sufficiently high trust scores. The overall attack success probability under the adaptive fusion regime was reduced to a level that satisfies high-assurance access control requirements.

Table 1. Comparative Authentication Performance of Different Biometric Configurations

Authentication Model	False Acceptance Rate (FAR)	False Rejection Rate (FRR)	Equal Error Rate (EER)	Attack Detection Rate
Physical only	0.021	0.014	0.017	0.72
Behavioral only	0.028	0.036	0.032	0.81
Static multimodal	0.013	0.018	0.015	0.89
Adaptive multimodal	0.008	0.012	0.010	0.94

The adaptive multimodal model achieved the lowest equal error rate and the highest attack detection rate. The improvement in attack detection is particularly significant in scenarios involving combined physical and behavioral deception, which represent a realistic threat in modern adversarial environments. Analysis of trust score trajectories revealed that adaptive weighting between physical and behavioral components played a decisive role in stabilizing decision outcomes. During periods of normal, low-variance interaction, the model assigned greater weight to behavioral evidence, increasing sensitivity to subtle deviations. When behavioral variance increased, for example due to unfamiliar input devices, the model automatically shifted emphasis toward physical biometrics. This dynamic rebalancing

prevented excessive false rejections without sacrificing attack sensitivity.

The observed trust score distributions remained well separated between legitimate and illicit access attempts throughout the study. No progressive collapse of class margins was detected, which indicates that the continuous adaptation mechanism does not induce threshold drift toward unsafe operating regions. The results confirm that adaptive multi-feature fusion provides a quantitatively and qualitatively superior basis for biometric authentication in dynamic operational environments. The next section will interpret these findings in the broader context of biometric security research and examine the specific role of the patented multi-level architecture in enabling these performance gains.

Discussion

The results of this study provide empirical confirmation that adaptive multi-feature biometric fusion constitutes a fundamentally more resilient approach to authentication than both unimodal and static multimodal configurations. The observed improvements are not merely incremental but structural in nature, reflecting the systemic advantages of continuous learning, dynamic trust modeling, and cross-modal compensation between physical and behavioral evidence. These findings align with the broader theoretical trajectory of biometric research, which increasingly emphasizes the shift from isolated trait verification toward integrated, risk-aware identity assessment [11,13]. A central implication of the results concerns the inherent limitations of static biometric thresholds. In conventional systems, fixed decision boundaries impose a rigid trade-off between security and usability that cannot accommodate natural behavioral evolution or abrupt contextual change. The adaptive thresholding mechanism employed in the proposed model resolves this tension by transforming authentication into a dynamic control process.

The experimentally observed stability of false rejection rates under behavioral drift directly reflects the capacity of the reinforcement learning module to recalibrate internal reference distributions without eroding impostor discrimination. This feature is particularly salient for long-term deployments in enterprise and critical infrastructure environments, where authentication systems must operate reliably over months and years without frequent manual reconfiguration. The role of behavioral biometrics within the fusion framework deserves special attention. When applied in isolation, keystroke and mouse dynamics exhibit significant sensitivity to device properties, cognitive load, and transient physiological states. These properties explain the comparatively elevated false rejection rates observed in the unimodal behavioral condition. However, when embedded within the adaptive fusion architecture, behavioral traits cease to function as brittle primary authenticators and instead become high-resolution anomaly detectors. They provide continuous low-latency evidence that enhances the temporal granularity of trust assessment while remaining anchored to the stable identity confirmation supplied by physical biometrics. This dual function is precisely what enables the adaptive model to simultaneously achieve high attack detection rates and low usability penalties.

Conclusion

This study developed and empirically validated a practical implementation model of adaptive biometric authentication based on multi-feature fusion of physical and behavioral traits. The results demonstrate that neither physical nor behavioral biometrics alone can satisfy the security and usability demands of modern high-risk digital environments. Static fusion improves robustness only to a limited extent, as it fails to accommodate long-term behavioral drift and evolving adversarial strategies. The core contribution of the model lies in the integration of heterogeneous biometric evidence within a continuously learning decision framework. The experimental analysis showed that adaptive reweighting of physical and behavioral components stabilizes trust estimation under nonstationary interaction conditions and preserves class separation between legitimate users and attackers over extended operational periods. The observed increase in attack detection rate under combined replay, spoofing, and imitation scenarios confirms that cross-modal coupling significantly elevates the adversarial cost required to bypass authentication.

From a broader security perspective, the composite trust score mechanism developed in this work aligns naturally with zero-trust security principles, in which identity assurance is treated as a continuous, probabilistic process rather than a one-time verification event. Adaptive biometric fusion therefore should be viewed as a foundational technology for next-generation identity infrastructures in finance, healthcare, critical infrastructure, and large-scale enterprise systems.In conclusion, adaptive multi-feature biometric authentication represents a technically mature and conceptually robust pathway toward sustainable, high-assurance digital identity protection. The integration of physical and behavioral biometrics within a self-learning trust framework, as demonstrated in this study and embodied in the referenced patented system, provides a scalable foundation for secure access control in the face of rapidly evolving cyber threats.

References

1. Gaw S, Felten EW. Password management strategies for online accounts. SOUPS 2006 Proceedings. 2006. 44-55.
2. Florencio D, Herley C. A large-scale study of web password habits. WWW 2007 Proceedings of the 16th International World Wide Web Conference. 2007. 657-666.
3. Ratha NK, Connell JH, Bolle RM. Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal. 2021. 40: 614-634.
4. Galbally J, Gomez-Barrero M, Fierrez J, Ortega-Garcia J. A review of biometric antispoofing. IEEE Signal Processing Magazine. 2012. 29: 1-13.
5. Marcel S, Nixon M, Fierrez J, Evans N. Handbook of biometric anti-spoofing (2nd ed.). Springer. 2019.
6. Monrose F, Rubin AD. Keystroke dynamics as a biometric for authentication. Future Generation Computer Systems. 2020. 16: 351-359.
7. Killourhy KS, Maxion RA. Comparing anomaly-detection algorithms for keystroke dynamics. DSN 2019 Proceedings. 2019. 125-134.
8. Fukushima M, Yamada Y, Kato T. Continuous user authentication using mouse dynamics. Computers & Security. 2019. 80: 97-111.

9. Ross A, Jain AK. Information fusion in biometrics. Pattern Recognition Letters. 2023. 24: 2115-2125.
10. Poh N, Bengio S, Korczak J. A multi-sample multi-source model for biometric authentication. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2010. 32: 1807-1814.
11. Jain AK, Ross A, Nandakumar K. Introduction to biometrics (2nd ed.). Springer. 2016.
12. Meng W, Wong D, Furnell S, Zhou J. Surveying the development of biometric user authentication on mobile phones. IEEE Communications Surveys & Tutorials. 2020. 17: 1268-1293.
13. Rattani A, Scheirer W J, Ross A. Open-set recognition in biometric systems: A review. IEEE Access. 2020. 8: 140344-140360.