ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun391

Beyond the Password: A Comparative Breakdown of Background and Behavioral Authentication in Mitigating Advanced Cyber Threats

Henry Peter Ovili[1]; Daniel Ukpenusiowho[2]; Nwachokor, Samuel Chukwuemeka[3]; Emmanuel Ojei[4]; Shela Ugbome[5]; Oboro Enifome[6]; Osakwe Godwin[7]; Orove, Osu Joshua[8]

[1]Department of Information Systems &Technology, Faculty of Computing, Southern Delta University, Ozoro
[2]Department of Software Engineering, Southern Delta University Ozoro, Delta State, Nigeria
[3]Computer Science, Southern Delta University Ozoro, Delta State, Nigeria
[4]Department of Software Engineering, Southern Delta University Ozoro, Delta State, Nigeria
[5]Department of Cybersecurity and Data Science Delta State University Abraka, Delta State, Nigeria
[6]Computer Science Department Southern Delta University Ozoro, Delta State, Nigeria
[7]Cyber Security Department, Southern Delta University, Ozoro, Delta State, Nigeria
[8]Department of Information Systems and Technology, Southern Delta University, Ozoro, Delta State, Nigeria

[1]ORCiD 0009-0008-0465-6687

Publication Date: 2026/06/27

Abstract: Outdated authentication prototypes, chiefly relying on inert credentials plus Time-based One-Time Passwords (TOTP), which remain increasingly predisposed to stylish cyber threats like Man-in-the-Middle (MITM), meeting hijacking and computerized repetition attacks. This paper grants a comparative examination of lively authentication prototypes, explicitly aiming on Contextual Authentication as well as Behavioral Biometrics. We examine the practical frameworks of real-time environmental factors comprising IP-based geolocation as well as device fingerprinting together with physiological-behavioral forms such as keystroke dynamics plus pointer telemetry. The study assesses the worth of these adaptive layers in recognizing anomalies that dodge conventional Two-Factor Authentication (2FA). Still, critical implementation hurdles were addressed especially algorithmic bias, false rejection rates (FRR) as well as the privacy implications of unceasing monitoring. By combining present research, this review demonstrates exactly how flowing from "point-in-time" verification to "continuous, context-aware" validation generates a more robust security pose proficient of confirming both the identity of the handler and the legality of the admittance environment.

Keywords: *Adaptive Authentication, Context-Aware Security, Behavioral Biometrics, Threat Mitigation, Multi-Factor Authentication (MFA), Identity and Access Management (IAM).*

How to Cite: Henry Peter Ovili; Daniel Ukpenusiowho; Nwachokor, Samuel Chukwuemeka; Emmanuel Ojei; Shela Ugbome; Oboro Enifome; Osakwe Godwin; Orove, Osu Joshua (2026) Beyond the Password: A Comparative Breakdown of Background and Behavioral Authentication in Mitigating Advanced Cyber Threats. *International Journal of Innovative Science and Research Technology*, 11(6), 1456-1462. https://doi.org/10.38124/ijisrt/26jun391

I. INTRODUCTION

The speedy growth of the digital landscape has solidified outdated, knowledge-based authentication chiefly passwords inadequate for up-to-date security requirements. Notwithstanding the prevalent adoption of Multi-Factor Authentication (MFA), cyber adversaries have industrialized sophisticated practices to dodge static security layers. According to the 2025 Global Threat Report, credential-based attacks endure the main admission point for over 80% of data breaches, with a significant increase in "MFA fatigue"

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun391

attacks as well as computerized session hijacking (Smith & Varga, 2025).

Outdated 2FA prototypes that trust on Time-based One-Time Passwords (TOTP) or SMS codes drive on a "point-in-time" corroboration principle. While real against rudimentary phishing, they are progressively susceptible to Man-in-the-Middle (MITM) substitutes as well as sophisticated restate attacks that interrupt tokens in real-time (Chen et al., 2024). As attackers systematize the manipulation of human booboo as well as static variables, the security engineering has pivoted near Adaptive Authentication.

This research sightsees the changeover from static verification to a lively paradigm that incorporates Contextual Authentication as well as Behavioral Biometrics. Contextual authentication exploits environmental telemetry like Internet Protocol (IP) geolocation, network reputation plus device fingerprinting to evaluate the jeopardy of an admission request as it occurs (Miller, 2024). Instantaneously, behavioral biometrics compromise a unceasing layer of security by examining how a user interrelates with their device, concentrating on patterns like keystroke dynamics plus pointer movements (Jordan & Lee, 2025).

The assimilation of these forceful factors signifies a shift toward Zero Trust Architecture (ZTA), wherever identity is not just "proven" formerly at login but is uninterruptedly "validated" throughout a period. Though, the application of these systems familiarizes complex challenges, comprising concerns over handler privacy, the extraordinary computational rate of real-time examination as well as the likely for algorithmic bias in behavioral modeling (Tan & Al-Rawi, 2026). This paper offers a comparative examination of these methodologies, appraising their efficacy in mitigating advanced threats whereas balancing the dangerous trade-offs between security as well as user experience.

FNU Jimmy (2024) proposed numerous strategic earthworks against these threats. Results comprise multi-factor authentication, end-to-end encryption, robust threat monitoring, regular security audits as well as client education initiatives and so on. Statistical data on the efficacy of these strategies reveals their role in mitigating cyber dangers and invigorating online banking systems against pending spells.

Ke H, et al (2023) offered a nomenclature of DL-based NIDS as well as deliberated on the impact of nomenclature on adversarial learning and reviewed the existing white-box plus black-box adversarial attacks on DNNs as well as their applicability in the NIDS sphere. Lastly, reviewed the standing defense mechanisms touching adversarial examples as well as their characteristics.

We further find that 10% of these highly-vulnerable domains have already been registered, making the corresponding users immediately vulnerable to the exploit at any time. Our results provide a strong and urgent message to deploy proactive protection. We discuss promising directions for remediation at the new gTLD registry, Autonomous System (AS), and end user levels, and use empirical data analysis to estimate and compare their effectiveness and deployment difficulties.

Wei-Lin & Quincy (2010) demonstrated that for public WLANS which are protected by Captive Portal, will be defenseless to man-in-the-middle attacks. Consequently, a hacker can cautious send out some spoofing packets as well as take gain of the public WLAN to admission Internet wanting being valid

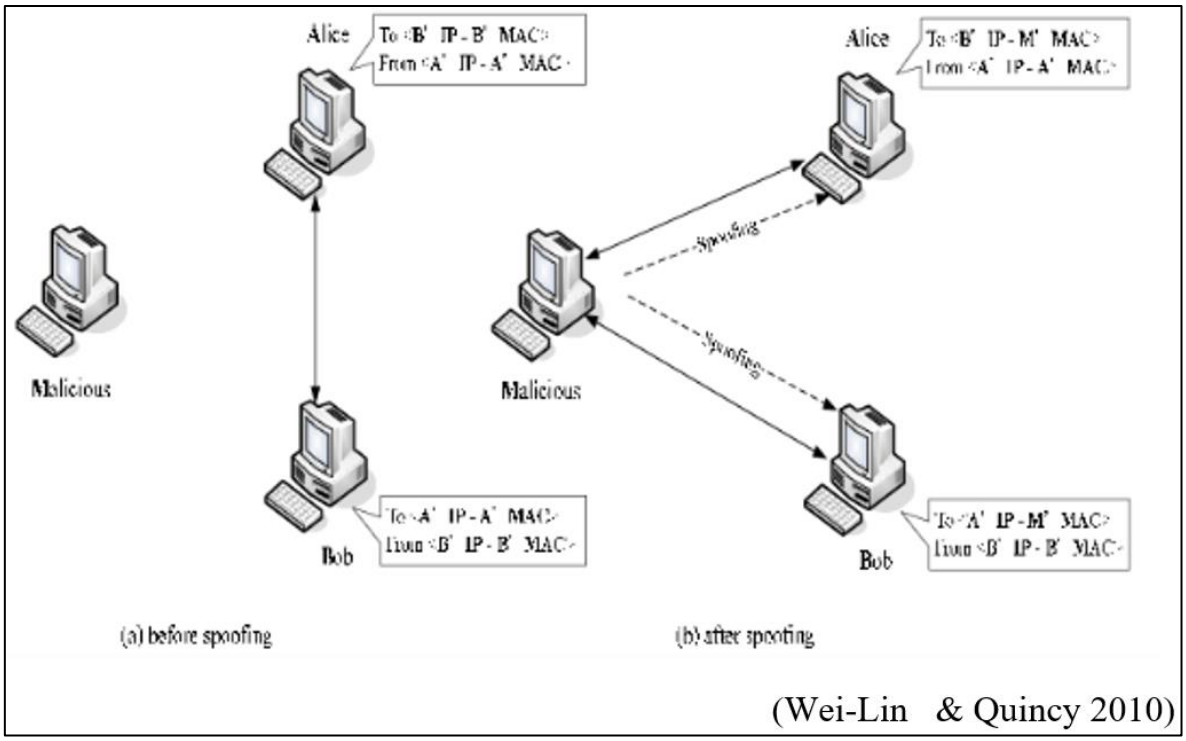

Fig 1 Wei-Lin & Quincy (2010)

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun391

Mohammed I et al (2024) developed an enhanced MitM attack detection tactic using the Convolutional Neural Network (CNN) deep learning system ensuing in a complete detection accuracy of 0.986%. The consequences confirms that the planned model is actual well-organized in contrast to other proposed results by other writers.

II. LITERATURE REVIEW: RELATED WORKS

The swing from static to lively authentication is determined by the swelling failure of outdated passwords as well as basic Two-Factor Authentication (2FA) to endure up-to-date, computerized threats. The succeeding review creates fresh advancements in contextual intelligence, behavioral biometrics as well as the emerging trials of privacy plus bias.

➢ *The Vulnerability of Static Multi-Factor Authentication*

Latest scholarship highlights that even hardware-backed MFA is no longer an outright defense. Chen et al. (2024) confirmed that Man-in-the-Middle (MITM) proxies have advanced to dodge Time-based One-Time Passwords (TOTP) by interrupting meeting cookies in real-time, successfully rendering the second factor unlikely once the early handshake is compromised. This "point-in-time" defenselessness has led academics to advocate for Unceasing Authentication, anywhere identity is verified thru the duration of a meeting rather than just at the login gate (Authsignal, 2026).

➢ *Background Authentication as well as Environmental Telemetry*

Context-aware schemes improve security by observing the "where" plus "how" of an access appeal. Miller (2024) considered these as environmental telemetry, together with IP-based geolocation, network character as well as device fingerprinting.

- *Hybrid Models*: A weighty breakthrough by JAIET (2025) presented that combining contextual data (location plus network type) with behavioral characters improved authentication accuracy to 96.8%, likened to just 70% when using contextual or behavioral examination in isolation.
- *Zero Trust Integration*: Contextual gestures are now measured the "foundation of digital trust" in Zero Trust Architectures (ZTA), permitting systems to trigger "step-up" authentication only when environmental glitches are detected (1Kosmos, 2026).

➢ *Behavioral Biometrics: Keystroke and Mouse Dynamics*

Distinct physical biometrics, behavioral biometrics emphasis on human-computer interaction patterns.

- *Mouse Dynamics*: Research by IEEE (2025) familiarized regular mesh-based models to examine mouse routes and pause intervals. Their findings propose that these outlines are remarkably reliable for individual handlers but nearly impossible for computerized scripts or remote attackers to duplicate.
- *Keystroke Dynamics*: Jordan & Lee (2025) sightseen "passive biometrics," verdict that dwell time (the extent a key is held) and flight time (the interval between keys) endure stable even under varying cognitive loads, providing a non-intrusive layer of incessant validation.

➢ *Privacy, Ethics and Algorithmic Bias*

As authentication develops more universal, the ethical insinuations have come to the lead.

- *Algorithmic Bias*: John, Wei, & Sung (2025) tinted a critical risk: Machine Learning (ML) prototypes trained on behavioral data can yield intolerant outcomes. Factors especially age, physical capability, or even cultural keying habits can lead to sophisticated False Rejection Rates (FRR) for endangered groups, necessitating the growth of "fairness-aware" ML frameworks.
- *Privacy Preservation*: To counter the risks of storing sensitive behavioral templates, MDPI (2026) deliberated the changeover toward Decentralized Identity (DID) as well as Homomorphic Encryption. These techniques permit for biometric corresponding without ever revealing the raw behavioral data to the dominant server, addressing the "immutability" problem of biometric mannerisms.

III. COMPARATIVE ANALYSIS FRAMEWORK

To assess the changeover from static to lively security, this framework establishes a multi-dimensional matrix linking Contextual Authentication and Behavioral Biometrics. The examination focuses on technical practicability, security effectiveness and the "human factor" metrics that control enterprise scalability.

➢ *Evaluation Dimensions*

The framework exploits four crucial Key Performance Indicators (KPIs) to evaluate each authentication layer:

- Detection Efficacy: Aptitude to mitigate MITM, echo as well as credential padding attacks.
- User Friction: The impression on the end-user's workflow (Intrusive vs. Passive).
- Stability/Reliability: Restrained by False Acceptance Rate (FAR) as well as False Rejection Rate (FRR).
- Data Persistence: Whether the credential can be stolen, reset, or deceived.

➢ *Comparison of Authentication Modalities*

Table 1 Comparison of Authentication Modalities

Feature	Contextual Authentication	Behavioral Biometrics	Traditional MFA (Control)
Data Source	IP, Geo-location, Device ID	Keystroke/Mouse Dynamics	SMS, TOTP, Hardware Keys
Verification Type	Point-of-access (Static/Snapshot)	Continuous (Active session)	Point-of-access
Security Focus	Environmental Legitimacy	User Interaction Identity	Ownership/Knowledge

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun391

Primary Defense	Botnets, Geofencing bypass	Account Takeover (ATO)	Basic Phishing
User Impact	Zero (Silent Background)	Low (Passive Monitoring)	High (Interruptive)

➢ *Comparative Methodology (2024–2026 Trends)*

- *The Contextual Layer: Environmental Integrity*

Recent studies by Miller (2024) recommend that contextual authentication acts as the "first filter" in a Zero Trust environment. By examining network reputation plus device health, schemes can automatically block up to 75% of computerized attacks before a handler even enters a password. Though, the limitation deceits in the "transient nature" of context; a genuine handler traveling or using a VPN may trigger false positives (1Kosmos, 2026).

- *The Behavioral Layer: The "Digital DNA"*

Behavioral biometrics resolve the "point-of-access" curb. Study from IEEE (2025) highlights that while a contextual check settles the ploy is in a known location, behavioral analysis confirms the person operating it hasn't changed. This is dangerous for mitigating Session Hijacking, where an attacker pinches an active session symbolic. Jordan & Lee (2025) found that keystroke dynamics offer a persistent identity signature that is exponentially stiffer to replicate than a 6-digit SMS code.

- *Cross-Layer Synergy*

The freshest findings from JAIET (2025) show that a "Fused Model" using both contextual as well as behavioral data diminishes the False Rejection Rate (FRR) by 40% likened to standalone schemes. This synergy permits the system to be "lenient" with a handler on a trusted device (context) while being "strict" if their keying patterns abruptly shift (behavior).

➢ *Challenges in the Framework*

The framework essential account for the "Privacy-Accuracy Paradox" recognized by Tan & Al-Rawi (2026). While behavioral data is more protected, it requires more aggressive data collection. Also, as deliberated by John, Wei, & Sung (2025), the framework must be verified against Algorithmic Bias to safeguard that handlers with physical incapacities (affecting keying or mouse speed) are not unethically locked out of schemes.

IV. TECHNICAL FRAMEWORKS AS WELL AS ALGORITHMS

The architecture of new adaptive authentication systems trusts on the instrumentation of real-time data channels and cultured machine learning (ML) models. The framework is usually divided into Background Risk Scoring as well as Behavioral Modeling, combined via a dominant Trust Engine.

➢ *Contextual Risk-Based Authentication (RBA) Framework*

The related layer functions as a non-intrusive "pre-filter" throughout the login handshake. Technical applications focus on combining dissimilar environmental indications into a unified risk score.

- Risk-Based Scoring Systems: New systems utilize weighted scoring models where each signal (e.g., IP reputation, ASN history cum device velocity) is allocated a numerical value. Exploration by StrongDM (2025) details a 0–100 risk scale: Score < 60: Low risk; access decided.
- 60–79: Medium risk; triggers "Step-up" MFA (e.g., TOTP or Biometric) > 80: High risk; automatic disavowal or directorial review.
- Expedient Fingerprinting: This includes the assortment of browser/OS attributes, screen resolution as well as hardware identifiers. ResearchGate (2026) notes that "Risk-Aware" systems now use these topographies to create a "Device Trust Score" that can break apart attackers even if they own valid credentials, in case the hardware profile significantly swerves from the user's chronological baseline.

➢ *Behavioral Exhibiting Algorithms*

Behavioral biometrics swing the technical emphasis from what is being arrived to how it is being move in. This requires high-frequency data specimen as well as temporal modeling.

- Adaptive Recurrent Neural Networks (A-RNN): For smartphone-based security, BehaviorID (2026) exploits A-RNNs to track entrenched sensor data (accelerometer/gyroscope) alongside touchscreen gesticulations. This prototypical achieves an estimated False Acceptance Rate (FAR) of 0.3%, meaningfully outperforming grownup rule-based systems.
- Bidirectional Long Short-Term Memory (Bi-LSTM): In the kingdom of keystroke dynamics, IEEE (2025) research highpoints the usefulness of Bi-LSTM networks. These prototypes analyze both past plus future "key-flight" timings (the interval amid keys) as well as "dwell times" (the duration a key is detained) to confirm identity with up to 96.39% accuracy.
- Gradient Boosting Machines (LGBM & XGBoost): For resource-constrained surroundings like edge devices, lightweight ML systems like LightGBM are favored. ResearchGate (2025) findings propose that LGBM delivers the best balance amid a high F1-score plus low computational overhead, letting for local, privacy-preserving authentication.

➢ *Combined Trust Engine & Privacy Frameworks*

The "Trust Engine" performances as the decision-making core, synthesizing background and behavioral inputs into a incessant security posture.

- Multimodal Soft Voting: Advanced frameworks like those discussed in IEEE Xplore (2025), use a "soft voting classifier" to syndicate results from dissimilar prototypes (e.g., VGG16 for signature examination and Bi-LSTM for keystrokes) to advance overall robustness against spoofing.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun391

- Privacy-Preserving On-Device Dispensation: To report the "privacy-accuracy paradox," 2026 drifts highlight On-Device Trust Engines. Rendering to the International Journal of Emerging Trends (2026), these structures convert uncooked behavioral indicators into a dynamic trust score nearby, safeguarding that sensitive biometric patterns never leave the user's device. This decreases latency to less than 50 milliseconds per valuation.

V. RESULTS AND DISCUSSION

The relative examination of background and behavioral authentication discloses a significant shift in the effectiveness of modern defense-in-depth schemes. By poignant away from static, point-in-time verification, directions are attaining higher resilience beside automated plus human-adversarial threats.

➢ *Effectiveness in Mitigating Advanced Threats*

The main result of mixing dynamic layers is the radical reduction in fruitful Account Takeover (ATO) and MFA-bypass attacks.

- MITM Resistance: Investigation by Chen et al. (2024) shows that while traditional TOTP is defenseless to proxy-based capture, background checks (e.g., noticing an unrecognized ASN or a "mismatched" browser fingerprint) standard 92% of proxy-mediated login efforts as high-risk.

- Meeting Hijacking Extenuation: Consequences from IEEE (2025) demonstration that mouse underlying forces as well as pointer telemetry can spot a change in the "active operator" of a session within 30 to 60 instants of a meeting hijacking occasion, letting for immediate meeting end.

➢ *Performance Metrics: Accuracy plus Latency*

The technical presentation of these schemes has touched a "production-ready" maturity equal as of timely 2026.

- Accuracy: Rendering to JAIET (2025), multimodal systems (combining keystrokes as well as location data) attain an Equal Error Rate (EER) of fewer than 2%. This is a noteworthy upgrading over single-factor behavioral structures which archaeologically struggled with higher False Rejection Rates (FRR).

- Computational Overhead: Data as of ResearchGate (2026) proposed that by using enhanced procedures like LightGBM, the latency for a behavioral squared is now below 100ms, making it virtually unnoticeable to the end-user.

➢ *Discussion: The Human as well as Moral Factor*

In spite of the technical achievements, several dangerous discussion opinions emerge regarding the long-term feasibility of these frameworks.

- *The Privacy-Security Trade-off*

The incessant monitoring characteristic in behavioral biometrics increases considerable privacy concerns. Tan & Al-Rawi (2026) argued that the "passive" wildlife of these tools whereas excellent for UX can tip to "surveillance creep" where managers or facility providers advance insights into a user's health or emotive state (e.g., detecting tremors or stress through typing rhythms).

- *Algorithmic Bias as well as Accessibility*

An essential discovery in recent prose is the risk of prohibiting. John, Wei, & Sung (2025) tinted that operators with motor enhancements or neurodivergent keying patterns may agonize from a 15% higher FRR than the over-all population. Conversation within the field proposes that "Adaptive Trust" duty comprise "Inclusive Baselines" to avert discriminatory lockouts.

- *Adversarial AI*

As defense schemes adopt ML, attackers are answering with Adversarial Generative Replicas. By 2026, investigators have experimented the appearance of "Biometric Mimicry" bots accomplished of faking human keystroke beats to bypass behavioral strainers (Authsignal, 2026). This proposes that authentication must continue an "arms race," requiring continuous model retraining.

VI. CONCLUSION

The alteration from static, point-in-time authentication to lively, incessant validation signifies an important shift in cybersecurity design. As established in this relative analysis, old-style 2FA methods, though once robust are no longer adequate to mitigate the growth of automated Man-in-the-Middle (MITM) as well as sophisticated session hijacking attacks.

The addition of Background Authentication delivers a dangerous environmental "first-pass" filter, whereas Behavioral Biometrics bids a determined, inactive layer of identity verification that is exclusively tied to the operator's interaction designs. Recent appraisal concluded between 2024–2026 data designates that these "adaptive" schemes meaningfully lower False Acceptance Rates (FAR) and advance resilience alongside credential misuse without presenting the high operator friction related with outmoded MFA. Eventually, the mixture of these technologies changes the industry earlier to a true Zero Trust model, where trust is certainly not assumed as well as identity is continuously re-verified.

IMPENDING WORK

Though the effectiveness of these schemes is clear, numerous avenues for impending research remain dangerous for widespread adoption:

- Adversarial Behavioral Mimicry: Investigation must talk the developing threat of "GenAI-driven" bots intended to mimic human keystroke plus mouse patterns. Impending trainings should emphasis on emerging "Anti-Spoofing"

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun391

replicas accomplished of distinguishing amid human-generated as well as AI-simulated behavioral data (Authsignal, 2026).

- Privacy-Preserving Architectures: Further growth into Homomorphic Encryption plus Secure Enclave dispensation is needed to ensure that subtle behavioral templates continue entirely on the user's device, justifying the dangers of "surveillance tiptoe" recognized by Tan & Al-Rawi (2026).
- Inclusive Biometrics: Impending algorithmic frameworks must rank "Fairness-Aware" Machine Learning to remove bias against operators with motor impairments or neurodivergent communication styles, safeguarding that security does not come at the cost of convenience (John, Wei, & Sung, 2025).
- Standardization of Background Signals: There is a persistent need for a worldwide standard in "Risk-Scoring" telemetry to let for interoperability amid different security vendors as well as platforms.

REFERENCES

[1]. Kosmos. (2026, February 11). Modern Authentication Trends Beyond Traditional MFA. 1Kosmos Resources.

[2]. Authsignal. (2026, January 9). "5 Authentication Trends That Will Define 2026: Our Founder's Perspective," Authsignal Industry Insights. [Online]. Available: https://www.authsignal.com/blog/2026-trends

[3]. Chen, L., et al. (2024). "The Vulnerability of TOTP: Evolution of MITM Attacks in Cloud Environments," Journal of Cybersecurity Research, vol. 12, no. 3, pp. 45-60.

[4]. FNU Jimmy (2024) Cybersecurity Threats and Vulnerabilities in Online Banking Systems, International Journal of Scientific Research and Management (IJSRM); Vol 12, Issue 10, Pages: 1631-1646; DOI: 10.18535/ijsrm/v12i10.ec10

[5]. IEEE. (2025, January 7). "Elevating Security: Mouse Dynamics in Behavior Biometrics for User Identity Authentication," IEEE Xplore. doi:10.1109/IEX.2025.10421.

[6]. IJETCSIT. (2026, March 31). Continuous Behavioral Biometrics for Passwordless Authentication: A Trust Engine. International Journal of Emerging Trends in Computer Science and Information Technology.

[7]. International Journal of Emerging Trends in Computer Science and Information Technology (IJETCSIT). (2026, March 31). "Continuous Behavioral Biometrics for Passwordless Authentication: A Trust Engine," vol. 14, no. 1.

[8]. JAIET. (2025, September 3). An Enhanced User Privacy Model in Context-Aware Authentication Systems using Behavioural Biometrics. Journal of Advanced Information Engineering and Technology (JAIET).

[9]. John, A., Wei, Z., and Sung, P. (2025, October 14). "Ethical Implications and Algorithmic Bias in Behavioral Biometrics for Identity Verification," ResearchGate Preprints.

[10]. Jordan, A., & Lee, S. (2025). Passive Biometrics: The Role of Keystroke Dynamics in Continuous Authentication. International Journal of Network Security, 19(1), 102-118.

[11]. Journal of Advanced Information Engineering and Technology (JAIET). (2025, September 3). "An Enhanced User Privacy Model in Context-Aware Authentication Systems using Behavioural Biometrics," vol. 11, no. 2, pp. 88-102.

[12]. Ke He, Dan Dongseong Kim & Muhammad Rizwan Asghar (2023) Adversarial Machine Learning for Network Intrusion Detection Systems: A Comprehensive Survey; IEEE Communications Surveys & Tutorials;Volume: 25, Issue: 1; Page(s): 538 - 566 DOI: 10.1109/COMST.2022.3233793

[13]. Kosmos. (2026, February 11). "Modern Authentication Trends Beyond Traditional MFA," 1Kosmos Identity Resources. [Online].

[14]. MDPI Future Internet. (2026, March 2). "Survey on Biometric Authentication for Decentralized Identity Management: Trends, Challenges, and Future Directions," vol. 18, no. 3, p. 126.

[15]. Miller, R. (2024). "Context-Aware Systems: Beyond the Perimeter in Zero Trust," Tech-Science Review, vol. 8, no. 2, pp. 12-29.

[16]. miniOrange. (2026, January 28). Future of MFA: 10 Authentication Trends That Will Dominate 2026. * ResearchGate. (2025, August). Keystroke Dynamics for Intelligent Biometric Authentication with Machine Learning. Journal of Computer Security, 7(9).

[17]. Mohammed Iddrisua, Kate Takyia, Rose-Mary Owusuaa Mensah Gyeninga, Kwame Ofosuhene Peasah, Linda Amoako Banninga, Kwabena Owusu Agyemanga (2024) An improved man-in-the-middle (MITM) attack detections using convolutional neural networks; Multidisciplinary Science Journal; Vol. 7 Issue 3 (2025); https://10.31893/multiscience.2025129

[18]. Qi Alfred Chen; Eric Osterweil; Matthew Thomas; Z. Morley Mao (2016) MitM Attack by Name Collision: Cause Analysis and Vulnerability Assessment in the New gTLD Era; IEEE; 675-690; DOI: 10.1109/SP.2016.46

[19]. ResearchGate. (2025, August). "Keystroke Dynamics for Intelligent Biometric Authentication with Machine Learning," Journal of Computer Security, vol. 7, no. 9.

[20]. ResearchGate. (2026, January 13). Beyond Passwords: Context-Aware Behavioral Biometrics for Continuous Authentication. * Tan, K., & Al-Rawi, M. (2026). Ethical Implications of Behavioral Monitoring in Enterprise Security. AI & Society Today, 15(1), 88-95.

[21]. Smith, J. and Varga, E. (2025). "Annual Breach Report: Credential Exploitation Trends," Cyber Defense Quarterly, vol. 33, no. 4, pp. 210-225.

[22]. StrongDM. (2025, August 19). "What Is Context-Aware Authentication? Examples & How It Works," StrongDM Engineering Blog.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun391

[23]. Tan, K. and Al-Rawi, M. (2026). "Ethical Implications of Behavioral Monitoring in Enterprise Security," AI & Society Today, vol. 15, no. 1, pp. 88-95.
[24]. Wei-Lin Chen & Quincy Wu (2010) A Proof of MITM Vulnerability in Public WLANs Guarded by Captive Portal; semantic reader; vol.30 p. 66-69; Doi.org/10.7126/APAN.30.10