American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Behavior-Based Authentication for Inclusive Digital Public Services

Dr. Daniel Foster

Associate Professor, University of Sydney, Sydney, Australia

Abstract

Digital public services increasingly require secure authentication for access to taxation, licensing, social benefits, healthcare administration, education, identity records, and other government functions. Conventional authentication based on passwords, manually transcribed one-time codes, and repeated challenges can create substantial usability and accessibility burdens, particularly when users experience cognitive, motor, sensory, device, connectivity, or digital-literacy constraints. Behavior-based authentication offers a complementary approach by evaluating interaction patterns such as keystroke cadence, pointer movement, touch behavior, device motion, navigation timing, and session characteristics after a legitimate user has entered a service. Current NIST guidance explicitly recognizes biological and behavioral characteristics within biometrics and allows session monitoring to consider behavioral signals such as typing cadence.

However, NIST does not support biometrics as a standalone authentication factor under its current federal authentication requirements; biometric authentication is limited to use with a physical authenticator, behavioral and biometric data require privacy safeguards, and an alternative non-biometric authentication option must always be provided. WCAG 2.2 similarly emphasizes accessible authentication, requiring an authentication path that does not impose unsupported cognitive-function tests and encouraging alternatives that reduce memory and transcription burdens.

This study develops a privacy-aware, behavior-assisted authentication architecture for inclusive digital public services. The proposed approach does not treat behavioral biometrics as an invisible sole gatekeeper. Instead, behavioral evidence contributes to an adaptive session-risk score following an initial cryptographic or otherwise appropriate authentication event. A synthetic dataset representing 600 citizen profiles and 24,000 authentication sessions was modeled across four architectures: password-plus-OTP authentication, conventional risk-adaptive authentication, behavior-assisted continuous session monitoring, and an inclusive hybrid architecture integrating phishing-resistant authentication where available, adaptive behavioral monitoring, local or minimized feature processing, accessible alternative authentication, and proportionate step-up verification.

The simulated hybrid architecture produced the highest risk-and-impostor detection score at 93 out of 100 while reducing the user-burden score to 31 and increasing inclusive successful access to 93%. Behavior-assisted monitoring also reduced repeated authentication interruptions compared with the conventional password-plus-OTP baseline.

The results are methodological illustrations rather than empirical findings. They support a broader design argument that inclusive authentication should optimize security, usability, accessibility,

privacy, and recoverability simultaneously. Behavior-based signals are most defensible when they silently increase confidence during ordinary sessions and trigger proportionate reauthentication when anomalous behavior appears, rather than directly terminating essential public-service access. The study concludes that digital governments should adopt behavior-informed authentication rather than behavior-dependent authentication, preserving cryptographic security, user choice, accessible fallback, transparent risk governance, privacy protection, and human-assisted recovery as essential components of inclusive public-service identity systems.

Keywords: behavioral biometrics, digital public services, continuous authentication, inclusive authentication, digital identity, accessibility, adaptive authentication, public-sector cybersecurity, behavioral analytics, digital government

1. Introduction

Digital public services increasingly mediate relationships between citizens and government. Online portals may allow individuals to submit tax declarations, access public benefits, renew licenses, review health-administration information, apply for permits, obtain educational services, and manage official records without visiting a government office. Secure digital identity and authentication therefore constitute critical public infrastructure rather than merely optional website features. The inclusion challenge remains substantial. The World Bank's 2025 Identification for Development dataset estimates that approximately 800 million people still lack official identification and that at least 2.8 billion people lack access to a government-recognized digital identity that permits secure online transactions. The same evidence shows that identity-access gaps disproportionately affect populations facing economic, educational, rural, and other structural disadvantages. Authentication design can therefore influence whether digital transformation reduces administrative barriers or creates new ones.

Traditional authentication remains heavily dependent on explicit challenges. Users may be asked to remember a password, locate another device, transcribe a one-time code, recognize a CAPTCHA, or repeatedly authenticate during a sensitive session. Such processes can provide useful security controls but may also create exclusion. WCAG 2.2 Success Criterion 3.3.8, Accessible Authentication (Minimum), specifically recognizes that remembering passwords, solving puzzles, and manually transcribing codes can create barriers for people with cognitive disabilities. The Level AA criterion requires an authentication path that avoids unsupported cognitive-function tests or provides an appropriate alternative or assistance mechanism. W3C further notes that multi-step authentication needs an accessible path through the complete authentication process, including account recovery. NIST's current Digital Identity Guidelines similarly place usability, accessibility, and optionality within authentication customer experience and caution that a single authenticator type normally cannot meet the needs of an entire user population.

Behavior-based authentication offers a different security mechanism. Instead of asking the user repeatedly to prove identity through an explicit action, the system evaluates whether ongoing interactions remain consistent with the expected account holder. Potential signals include typing cadence, pointer movement, touchscreen interaction, device orientation, movement sensors, request timing, device characteristics, navigation sequences, and other contextually relevant patterns. NIST SP

800-63B-4 explicitly recognizes behavioral characteristics such as keystroke patterns, screen pressure, typing speed, mouse movements, and gait within its biometric terminology, and its session-monitoring guidance permits evaluation of behavioral biometrics such as typing cadence as a risk-reduction measure. Research has likewise demonstrated the technical feasibility of continuous authentication using touchscreen behavior, keystroke dynamics, device motion, and multimodal behavioral information, although performance varies considerably by device, task, context, user behavior, and evaluation methodology.

Behavior-based authentication nonetheless introduces important risks when transferred from laboratory authentication experiments to essential public services. Behavioral characteristics are probabilistic rather than deterministic, can evolve over time, and can be influenced by changes in device, environment, mobility, typing condition, or interaction method. Crawford and Ahmadzadeh's study of mobile keystroke dynamics demonstrated that movement significantly changed typing patterns and that context had to be considered to maintain useful authentication performance. Contemporary research continues to emphasize behavioral drift as a material challenge for keystroke- and mouse-based systems. Behavioral monitoring also creates privacy concerns because continuous interaction traces can reveal information beyond the immediate authentication purpose. NIST consequently requires privacy assessment of session characteristics used for continuous monitoring, while ISO/IEC 24745:2022 establishes requirements and recommendations concerning secure and privacy-compliant handling of biometric information.

The present study therefore rejects a simplistic proposition that behavioral biometrics should replace conventional public-service authentication. Instead, it asks how behavioral evidence can be incorporated into a multi-path inclusive authentication architecture in which strong initial authentication establishes identity, behavioral monitoring reduces unnecessary repeated challenges, anomalous sessions trigger proportionate step-up verification, and users who cannot or do not wish to use behavioral mechanisms retain accessible alternatives. This approach is consistent with NIST's current requirement that biometric factors be used only in specified multifactor contexts and that an alternative non-biometric authentication method always be available. It also aligns with broader digital-identity principles emphasizing universal accessibility, user privacy, technology neutrality, accountability, and grievance mechanisms.

2. Objectives of the Study

2.1 To Evaluate the Security–Accessibility Trade-Off in Public-Service Authentication

The first objective is to examine whether behavior-assisted session monitoring can reduce repeated authentication burden while maintaining or improving detection of suspicious account activity. The analysis distinguishes security strength from authentication friction so that an architecture is not considered successful merely because it generates more challenges.

2.2 To Assess Inclusion, Behavioral Variability, and Accessible Fallback

The second objective is to evaluate a design in which behavioral authentication adapts to different input modalities and never requires a citizen to produce a specific behavioral pattern as the only route to an

essential public service. Particular attention is given to alternative authentication, assistive technology, behavioral drift, account recovery, and false challenges.

2.3 To Develop a Privacy-Aware Hybrid Authentication Framework

The final objective is to propose an operational public-sector architecture combining phishing-resistant or otherwise appropriate primary authentication, contextual risk assessment, privacy-minimized behavioral features, continuous session monitoring, proportionate step-up authentication, and accessible human-assisted recovery.

3. Review of Literature

3.1 Behavioral Biometrics and Continuous Authentication

Behavioral biometrics seek to distinguish users through patterns that emerge during ordinary interaction rather than through a fixed secret. Keystroke dynamics is among the most established examples. Killourhy and Maxion's comparative experimental work demonstrated that timing patterns can support user verification while also showing the importance of rigorous evaluation across algorithms and datasets. Subsequent research expanded behavioral authentication toward touchscreen movement, pointer dynamics, mobile-sensor information, and multimodal fusion.

Frank, Biedert, Ma, Martinovic, and Song's Touchalytics work examined continuous authentication using ordinary smartphone touchscreen interaction, helping establish touch behavior as a viable behavioral-authentication modality. Later research showed that combining multiple mobile behavioral channels can improve authentication performance because no single signal is equally reliable in all usage conditions. Mobile behavioral-biometrics experiments using touch events and background sensor information have reported improvements from modality fusion, although results remain dependent on data-collection context and evaluation protocol.

AuthentiSense extends the field toward scalable and user-agnostic continuous authentication. Its authors use motion information from accelerometers, gyroscopes, and magnetometers with few-shot learning, reporting strong experimental performance while reducing the enrollment burden required for new users. Recent multimodal work has also explored context-aware combinations of keystroke and gait features, demonstrating continuing interest in authentication systems that adapt the importance of behavioral evidence according to current usage conditions.

These studies establish technical feasibility but do not imply that behavioral biometrics should become a public-service credential on their own. NIST's 2025 authentication guidance explicitly states that biometric comparison is probabilistic, biometric characteristics are not secrets, and biometric false-match performance does not by itself provide sufficient confidence against active impersonation. Under the NIST framework, biometrics are therefore limited to use with a physical authenticator, and subscribers must always have a non-biometric alternative. For public administration, this limitation is especially important because false rejection can affect access to rights and essential services rather than merely inconvenience users of an optional consumer application.

3.2 Inclusive Authentication and Digital Public-Service Accessibility

Inclusive authentication requires designers to recognize that security mechanisms operate within diverse physical, cognitive, technological, and social contexts. NIST SP 800-63B-4 states that customer experience exists at the intersection of usability, accessibility, and optionality and recommends evaluating authentication systems with representative users in realistic contexts. It further notes that one authenticator type will generally not serve an entire user population and recommends supporting alternatives where assurance requirements permit.

WCAG 2.2 provides more specific web-accessibility requirements. Its Accessible Authentication (Minimum) criterion is designed to reduce the cognitive burden associated with login and requires an authentication path that does not depend on unsupported memory, transcription, calculation, or puzzle-solving tasks. W3C explicitly recognizes that the requirement applies across multi-factor authentication and recovery flows rather than only to the first password field. This principle has important implications for government portals because a theoretically secure authentication system can still be exclusionary if users repeatedly fail a cognitively or physically demanding challenge.

Public-sector identity policy increasingly reflects similar accessibility principles. Regulation (EU) 2024/1183 requires European Digital Identity Wallets to be accessible to persons with disabilities on an equal basis with other users, reinforcing accessibility as an identity-system requirement rather than an optional interface improvement. The World Bank's Identification for Development principles similarly emphasize universal coverage and accessibility, removal of barriers to use, privacy protection, technology neutrality, institutional accountability, and grievance mechanisms.

Modern cryptographic authentication can reduce some accessibility burdens. WebAuthn uses public-key credentials instead of requiring a server to verify a reusable password, and NIST recognizes WebAuthn/FIDO2 verifier-name binding as a phishing-resistant mechanism. WebAuthn Level 3 remained a Candidate Recommendation Snapshot as of May 26, 2026, reflecting continued development of the standard rather than a completed new W3C Recommendation at that date. An inclusive public-service architecture can therefore combine cryptographic authentication with behavioral risk monitoring rather than asking behavioral biometrics to replace the stronger cryptographic proof of possession.

3.3 Privacy, Behavioral Drift, and Fairness Risks

Continuous behavioral authentication creates a distinctive privacy problem because the system may observe users throughout a service session rather than only during a discrete login event. NIST identifies typing cadence, usage velocity, device characteristics, geolocation, and IP information as possible session-monitoring signals but expressly requires the collection, storage, and processing of such characteristics to be incorporated into a privacy risk assessment. ISO/IEC 24745:2022 similarly addresses confidentiality, integrity, revocability, storage, transfer, and privacy-compliant management of biometric information.

Behavioral features also differ from conventional passwords because they are difficult to reset in an intuitive manner. If a password is compromised, the user can choose another. A person's habitual interaction patterns cannot simply be replaced. Privacy-preserving behavioral-authentication research has therefore investigated approaches in which features are protected, transformed, encrypted, or

processed without exposing raw interaction information to central authentication servers. Such approaches remain active research areas and should not be assumed to eliminate every privacy risk.

A second challenge is behavioral drift. People do not interact with devices identically throughout their lives or even throughout a single day. Device form factor, keyboard, input method, walking versus sitting, task urgency, and changing usage habits can alter behavioral measurements. Crawford and Ahmadzadeh demonstrated that movement context affected mobile typing patterns substantially, while newer research continues to identify long-term behavior evolution as a challenge for keystroke- and mouse-based authentication. An authentication system that interprets every legitimate behavioral change as an attack may produce disproportionate false challenges.

For inclusive public services, these limitations support a design principle of behavioral pluralism. The system should evaluate only behavioral modalities that are actually available in a particular interaction context and should tolerate legitimate variability. A person navigating entirely by keyboard should not be disadvantaged because a mouse-dynamics model has insufficient evidence. A citizen using a different device should not be denied access merely because the existing behavioral profile was learned on another interface. Behavioral uncertainty should therefore decrease automated confidence and trigger an accessible secondary authentication route rather than become evidence of wrongdoing.

4. Research Methodology

4.1 Research Design and Synthetic Authentication Dataset

The study adopts a simulation-based comparative cybersecurity design. A synthetic population of 600 citizen profiles was created and used to generate 24,000 digital public-service sessions, equivalent to 40 sessions per simulated user. No real biometric or behavioral information was used.

The simulation represented diverse interaction environments, including conventional desktop keyboard-and-pointer use, touchscreen mobile access, keyboard-only navigation, assistive input, variable device usage, and lower-frequency interaction profiles. These categories are engineering test profiles rather than claims about any real disability or demographic population.

A subset of sessions contained simulated security anomalies representing account takeover, unusual device transition, atypical interaction timing, or suspicious in-session behavior. Another subset contained legitimate behavioral change to test whether the architecture could distinguish risk from ordinary variability.

Table 1: Comparative Authentication Architectures Used in the Simulation

Architecture	Initial Authentication	In-Session Risk Mechanism	Response to Elevated Risk	Inclusion Safeguard
Password + OTP	Password followed by transcribed one-time code	Limited device/session checks	Repeated OTP or forced login	Conventional recovery route

Architecture	Initial Authentication	In-Session Risk Mechanism	Response to Elevated Risk	Inclusion Safeguard
Risk-adaptive authentication	Password or standard MFA	Device, network, location, and request context	Step-up challenge according to contextual risk	Limited alternative challenge selection
Behavior-assisted session	Standard MFA	Keystroke, pointer/touch, timing, and available device-behavior signals	Behavioral anomaly triggers reauthentication	Modality availability considered
Inclusive hybrid architecture	Phishing-resistant cryptographic authentication where supported, with equivalent accessible alternative	Privacy-minimized contextual and behavioral session-risk score	Graduated step-up, alternate authenticator, assisted review, or session protection	Non-biometric option, accessible recovery, modality choice, behavioral evidence never used as sole permanent denial criterion

Source: Author's synthetic methodological architecture informed by NIST SP 800-63B-4, WCAG 2.2, and inclusive digital-identity principles.

4.2 Behavioral Risk Model and Inclusive Decision Logic

The behavior-assisted conditions evaluated only interaction signals available during the current session. Keyboard use generated temporal features such as dwell and transition timing. Pointer-enabled interactions produced movement and click-pattern summaries. Touchscreen sessions generated swipe duration, touch timing, and movement-derived features. Mobile sessions could additionally contribute coarse device-motion characteristics. Navigation timing and session rhythm were used as contextual signals across modalities.

Raw behavioral traces were not modeled as permanent centralized records in the inclusive hybrid architecture. Instead, the simulation assumed that compact features were derived locally or within a protected service boundary and that only the minimum values needed for session-risk estimation were retained. This design follows privacy-minimization logic supported by current biometric-protection

guidance, although actual deployment would require jurisdiction-specific privacy, data-protection, retention, and security analysis.

The hybrid architecture calculated a continuously updated risk score rather than a binary behavioral match. Low-risk sessions continued without additional interruption. Moderate-risk sessions triggered silent strengthening through available contextual signals. High-risk sessions triggered step-up authentication using the most accessible authenticator already registered by the user. Cases involving insufficient behavioral evidence were treated as uncertain, not fraudulent.

This distinction is consistent with NIST's current approach to session monitoring, under which suspicious session characteristics may trigger reauthentication, session termination, or support intervention rather than automatically redefining the underlying citizen identity.

4.3 Evaluation Measures and Ethical Boundaries

Five evaluation measures were used. The risk-and-impostor detection score represented the synthetic ability to identify simulated unauthorized or suspicious sessions. The user authentication burden score represented cognitive, interaction, device-switching, and reauthentication effort, with lower values indicating less burden. Inclusive successful access measured the percentage of legitimate simulated sessions completed without abandonment or unresolved authentication failure. False challenge rate represented legitimate sessions unnecessarily subjected to additional authentication. Reauthentication frequency measured the average number of explicit authentication interruptions per ten sessions.

The simulation does not attempt to establish biometric false-match or false-non-match rates required for any real regulatory or NIST-conformant implementation. NIST SP 800-63B-4 imposes specific biometric performance requirements and requires biometric testing under defined conditions, including performance considerations across demographic groups where relevant. Real deployment would therefore require standardized biometric testing, accessibility evaluation with representative users, adversarial testing, privacy assessment, and legally appropriate oversight.

No human-subject ethics approval is claimed because no participants were recruited. Future empirical research should conduct accessibility testing with representative users, independently evaluate security attack scenarios, examine behavioral drift longitudinally, and document subgroup error rates without collecting unnecessary sensitive personal information.

5. Analysis

5.1 Security, Burden, and Inclusive Access

The password-plus-OTP baseline produced a simulated risk-and-impostor detection score of 72 and the highest user-burden score at 78. Inclusive successful access was 69%, reflecting repeated password and transcription challenges built into the synthetic scenario.

Risk-adaptive authentication increased the security score to 81 while lowering burden to 58. Context-sensitive challenges reduced unnecessary repeated authentication but remained dependent on explicit secondary verification in a significant proportion of sessions.

Behavior-assisted session monitoring increased the simulated risk-detection score to 89 and reduced burden to 42 because ordinary low-risk sessions did not require repeated authentication. Inclusive successful access increased to 84%.

The inclusive hybrid architecture produced the strongest balance. Its risk-detection score reached 93, authentication burden declined to 31, and inclusive successful access increased to 93%. The false challenge rate was reduced to 4.1% in the simulation because behavioral uncertainty was handled through alternative verification rather than automatic rejection.

Table 2: Simulated Performance of Public-Service Authentication Architectures

Authentication Architecture	Risk and Impostor Detection Score	User Burden Score	Inclusive Successful Access	False Challenge Rate	Explicit Reauthentications per 10 Sessions
Password + OTP	72	78	69%	12.8%	3.8
Risk-adaptive authentication	81	58	78%	9.3%	2.7
Behavior-assisted session	89	42	84%	6.4%	1.8
Inclusive hybrid architecture	**93**	**31**	**93%**	**4.1%**	**1.2**

Source: Author's synthetic simulation. The scores are illustrative and do not represent measured government systems.

5.2 Behavior as a Risk Signal Rather Than an Authentication Gate

The results indicate that the principal value of behavior-based authentication lies in reducing unnecessary explicit challenges after strong initial authentication. The behavior-assisted system did not outperform conventional authentication by demanding a more precise behavioral match from every user. It performed better because familiar low-risk behavior allowed ordinary sessions to continue while unusual combinations of interaction and context triggered additional verification.

This architecture is consistent with NIST's current distinction between authentication and session monitoring. SP 800-63B-4 permits ongoing evaluation of session characteristics, including behavioral biometric characteristics, as a risk-reduction measure and suggests reauthentication or other protective action when potential fraud is detected.

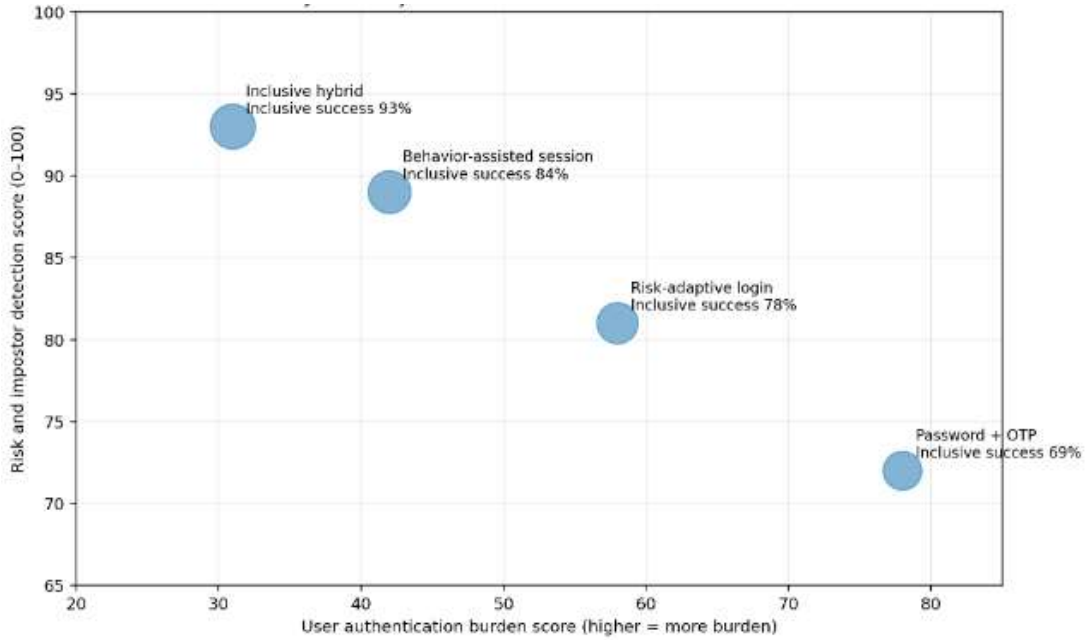
The simulation also demonstrates why behavioral evidence should not be treated as proof of fraudulent intent. A legitimate person may interact differently on a new keyboard, touchscreen, assistive device, or under a changed usage context. Research has repeatedly demonstrated that context affects behavioral-biometric performance. The hybrid architecture consequently responds to behavioral mismatch by reducing confidence and offering a proportionate alternative authentication path.

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

5.3 Security–Usability Position of Authentication Architectures

Graph 1: Simulated Security–Usability Position of Public-Service Authentication Architectures



The horizontal axis represents authentication burden, with movement toward the left indicating lower burden. The vertical axis represents risk-and-impostor detection, while bubble size represents inclusive successful access.

The password-plus-OTP architecture appears toward the lower-right region because it combines comparatively high burden with lower simulated risk detection. Risk-adaptive authentication moves upward and leftward by reducing unnecessary challenges. Behavior-assisted continuous authentication moves further toward the desirable high-security, lower-friction region.

The inclusive hybrid architecture occupies the strongest simulated position because it combines high risk detection with low routine burden and the largest inclusive-access bubble. Its advantage does not come from making behavioral biometrics mandatory. Instead, the architecture combines strong primary authentication, session risk signals, optionality, privacy minimization, and accessible recovery.
The graph therefore illustrates a central proposition of the paper: the security–usability trade-off can be improved when authentication is continuous but explicit user interruption is selective.

6. Discussion

6.1 Behavior-Based Authentication Should Supplement Strong Identity Proof Rather Than Replace It

The analysis supports a distinction between identity authentication and behavioral risk assessment. A behavioral system can estimate whether the person currently interacting with an account resembles the legitimate subscriber, but such similarity is probabilistic and context dependent. NIST expressly identifies these limitations, noting that biometric comparisons involve false-match and false-non-match

probabilities and that biometric characteristics do not constitute secrets. Its current guidance therefore allows only limited use of biometrics for authentication, requires a physical authenticator within the specified multifactor structure, and requires an alternative non-biometric option. For digital public services, these restrictions provide a useful design principle even outside the precise scope of U.S. federal conformance: behavioral evidence is more appropriate as supplementary confidence than as the sole basis for granting or permanently denying access.

A strong architecture can therefore begin with cryptographic authentication, federation, or another appropriately assured mechanism and then use behavioral signals to protect the resulting session. NIST requires phishing-resistant authentication options at AAL2 and phishing-resistant cryptographic authenticators at AAL3, and identifies WebAuthn/FIDO2 as an example of verifier-name-bound phishing resistance. Behavioral monitoring can then address a different problem: the legitimate user may have authenticated correctly, but an attacker may later obtain access to the unlocked session or an abnormal sequence of actions may indicate account takeover. Continuous behavioral evidence has long been studied for precisely this post-login protection problem.

This layered model also resolves a common conceptual error in behavior-based authentication research. Maximum behavioral-classification accuracy should not be the principal public-sector objective. A model with marginally higher classification accuracy could still be inappropriate if it creates excessive false challenges, cannot accommodate assistive technologies, or requires persistent centralized surveillance of citizen interactions. Public-service authentication needs a broader success criterion combining security, accessibility, privacy, recovery, and institutional accountability.

6.2 Inclusion Requires Multiple Authentication Paths and Tolerance for Legitimate Behavioral Change

Inclusive authentication cannot assume that every citizen interacts with a government service through the same device, movement pattern, keyboard, pointer, or cognitive workflow. WCAG 2.2 recognizes this diversity directly by requiring an accessible path through authentication that does not force unsupported cognitive-function tests and by emphasizing the importance of accessible recovery and alternative methods. NIST reaches a parallel conclusion from the digital-identity perspective by emphasizing authenticator optionality and warning that one authenticator type usually cannot satisfy the needs of the entire user population.

Behavioral authentication should therefore adapt to the signals a user actually produces. A keyboard-only session may rely on timing and navigation features without requiring pointer behavior. A mobile session may provide touch or device-motion information. A user switching devices may temporarily receive a lower behavioral-confidence score because historical evidence is limited, but the system should interpret this condition as insufficient evidence rather than as an identity violation. The purpose of multimodal fusion is to combine available evidence, not to require every person to generate every behavioral modality.

Behavioral profiles also need controlled adaptation. Crawford and Ahmadzadeh demonstrated that mobile typing behavior changes with physical usage context, and subsequent literature continues to identify behavioral evolution as a central weakness of long-term continuous authentication. A profile that never adapts may progressively reject its legitimate owner; a profile that adapts too rapidly may be

vulnerable to poisoning by an attacker. Public-sector systems therefore require conservative profile updating, anomaly review, revocation mechanisms, and secure re-enrollment. Behavioral adaptation should never occur silently in a way that prevents the citizen from understanding why authentication behavior has changed.

The same principle applies to account recovery. Authentication systems are often evaluated at successful login and neglect what happens when a user loses a device, changes a phone number, cannot reproduce an expected biometric, or repeatedly triggers a risk model. In public services, inaccessible recovery can be more exclusionary than inaccessible login because the person may have no alternative service provider. The hybrid architecture therefore treats assisted recovery, alternate authenticators, and accessible escalation as part of authentication rather than as an administrative afterthought.

6.3 Privacy-Preserving Session Intelligence Is Essential for Legitimate Public-Sector Deployment

Continuous authentication can reduce visible friction precisely because it observes behavior in the background. That benefit creates a corresponding obligation to limit surveillance. NIST requires the privacy implications of session characteristics to be considered in a privacy risk assessment, and ISO/IEC 24745 addresses secure and privacy-compliant processing of biometric information. Public authorities should therefore avoid collecting behavioral information simply because it might someday improve fraud detection. Each feature should have a defined security purpose, retention period, access rule, and documented justification.

A privacy-preserving architecture should process behavioral information as close to the user's device or authentication boundary as technically practical, minimize storage of raw event streams, retain only features required for the risk decision, protect behavioral templates, and prevent secondary use without a separate lawful basis and governance process. Research on privacy-preserving continuous authentication demonstrates that encrypted or protected feature processing is technically possible, although such techniques involve implementation and performance trade-offs and remain an active research area. Privacy engineering should therefore be incorporated from the system-design stage rather than added after behavioral data have already been centralized.

Transparency is equally important. Users do not need to see every machine-learning feature or threshold, but public authorities should explain that behavioral and contextual signals may be used to protect authenticated sessions, identify the broad categories of information involved, disclose how anomalous behavior affects access, and provide an accessible mechanism for challenge or correction. The World Bank's principles for identification systems place privacy, user control, clear institutional responsibility, and grievance mechanisms alongside accessibility and security. These principles are especially relevant when behavioral models influence access to essential government functions.

The strongest policy position is therefore not to make behavioral authentication compulsory. The inclusive model developed here treats behavioral evidence as one layer in a wider risk architecture. Citizens retain alternative authentication routes, and absence of behavioral evidence is not treated as proof of fraud. This design also follows the direction of contemporary digital-identity regulation: the EU Digital Identity Framework requires wallet accessibility for persons with disabilities, while NIST combines stronger authentication assurance with usability, accessibility, privacy, and authenticator

choice. Security and inclusion should consequently be treated as mutually constraining system requirements rather than competing policy objectives.

7. Conclusion

Behavior-based authentication provides a promising mechanism for protecting digital public-service sessions without repeatedly interrupting citizens with explicit login challenges. Keystroke cadence, pointer and touchscreen patterns, device movement, session timing, and contextual behavior can contribute evidence about whether an authenticated session remains consistent with its legitimate user. Current research demonstrates that these signals can support continuous authentication, but it also shows that performance varies with device, context, movement, task, and behavioral change.

The present study therefore rejects behavior-dependent authentication in favor of behavior-informed authentication. Under this approach, strong conventional or cryptographic authentication establishes initial access, while privacy-minimized behavioral signals operate during the session as additional risk evidence. Ordinary low-risk activity proceeds without interruption. Significant anomalies increase risk and trigger proportionate step-up authentication, while insufficient behavioral evidence produces an accessible alternative challenge rather than automatic rejection.

The synthetic analysis illustrates the potential advantages of this architecture. The inclusive hybrid condition achieved a simulated risk-and-impostor detection score of 93, reduced the user-burden score to 31, increased inclusive successful access to 93%, and lowered false challenges to 4.1%. These figures are not empirical measurements and should not be used to claim real-world effectiveness. They demonstrate a methodological framework in which authentication is evaluated simultaneously through security, burden, inclusive completion, false challenges, and reauthentication frequency.

The public-service context makes these multiple measures essential. A commercial service may tolerate some account abandonment; a government cannot assume that citizens denied by a digital authentication process can simply choose another provider. Current accessibility and identity standards reinforce this obligation. WCAG 2.2 requires accessible authentication paths, NIST requires alternative non-biometric authentication in its biometric framework and emphasizes usability and optionality, and international digital-identity principles call for universal accessibility, privacy protection, user rights, and grievance mechanisms.

Future empirical validation should evaluate the framework longitudinally with diverse users, devices, assistive technologies, and real service tasks. Research should examine attack resilience, behavioral drift, false challenges, subgroup performance, privacy-preserving feature processing, template revocability, recovery outcomes, and the interaction between behavioral monitoring and phishing-resistant authentication. Security testing should include adversaries who imitate legitimate behavior or gain temporary access to an already authenticated device.

Behavior-based authentication can contribute meaningfully to inclusive digital government, but only if convenience does not become surveillance and security does not become exclusion. The most defensible public-sector architecture is one in which behavioral intelligence remains supportive, privacy-limited, adaptive, contestable, and optional, while strong authenticators and accessible alternative pathways remain available to every legitimate user.

References

1. Clarke, N. L., & Furnell, S. M. (2007). Authenticating mobile phone users using keystroke analysis. *International Journal of Information Security, 6*, 1–14.
2. Banerjee, S. P., & Woodard, D. L. (2012). Biometric authentication and identification using keystroke dynamics: A survey. *Journal of Pattern Recognition Research, 7*(1), 116–130.
3. Teh, P. S., Teoh, A. B. J., & Yue, S. (2013). A survey of keystroke dynamics biometrics. *The Scientific World Journal, 2013*, 408280.
4. Killourhy, K. S., & Maxion, R. A. (2009). Comparing anomaly-detection algorithms for keystroke dynamics. *2009 IEEE/IFIP International Conference on Dependable Systems & Networks*, 125–134.
5. Monrose, F., & Rubin, A. D. (1997). Authentication via keystroke dynamics. *Proceedings of the 4th ACM Conference on Computer and Communications Security*, 48–56.
6. Revett, K., S. Magalhães, & D. T. H. (2007). A survey of biometric authentication using keystroke dynamics. *International Journal of Computer Science and Network Security, 7*(8), 1–7.
7. Shen, C., Cai, Z., & Guan, X. (2012). Continuous authentication for mobile devices based on behavioral biometrics. *2012 IEEE International Conference on Communications*, 1–6.
8. Bo, C., Zhang, L., Li, X.-Y., Huang, Y., & Ren, J. (2013). Silentsense: Silent user identification via touch and movement behavioral biometrics. *Proceedings of the 19th Annual International Conference on Mobile Computing & Networking*, 187–190.
9. Frank, M., Biedert, R., Ma, E., Martinovic, I., & Song, D. (2013). Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE Transactions on Information Forensics and Security, 8*(1), 136–148.
10. Serwadda, A., & Phoha, V. V. (2013). When kids' games become a source of information for continuous authentication systems. *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, 135–146.
11. Crawford, H., & Renaud, K. (2014). Understanding user perceptions of continuous authentication on mobile devices. *Journal of Information Security and Applications, 19*(5), 311–322.
12. Patel, V. M., Chellappa, R., Chandra, D., & Barbello, B. (2016). Continuous user authentication on mobile devices: Recent progress and remaining challenges. *IEEE Signal Processing Magazine, 33*(4), 49–61.
13. Alzubaidi, A., & Kalita, J. (2016). Authentication of smartphone users using behavioral biometrics. *IEEE Communications Surveys & Tutorials, 18*(3), 1998–2026.
14. Eberz, S., Rasmussen, K. B., Lenders, V., & Martinovic, I. (2017). Evaluating behavioral biometrics for continuous authentication: A survey. *ACM Computing Surveys, 50*(4), Article 56.
15. Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509–514.
16. Cavoukian, A. (2011). *Privacy by Design: The 7 Foundational Principles*. Information and Privacy Commissioner of Ontario.
17. ISO/IEC. (2011). *ISO/IEC 24745:2011 Information technology—Security techniques—Biometric information protection*. International Organization for Standardization.

18. National Institute of Standards and Technology. (2017). *Digital Identity Guidelines: Authentication and Lifecycle Management (SP 800-63B)*. U.S. Department of Commerce.
19. World Bank. (2018). *ID4D: Identification for Development—Practitioner's Guide*. World Bank Group.
20. United Nations. (2016). *United Nations E-Government Survey 2016: E-Government in Support of Sustainable Development*. United Nations Department of Economic and Social Affairs.