Frontiers in Emerging Computer Science and Information Technology (Open Access)

Volume 03, Issue 01, January 2026,
DOI: - https://doi.org/10.64917/fecsit/Volume03Issue01-01 PageNo.01-14

Biometric and Behavioral Authentication in IAM: Security, Privacy, and Continuous Verification Trade-offs

Kiran Kumar Puipati
Research Scholar, Department of Information Studies, Trine university, USA

RECEIVED - 11-20-2025, **RECEIVED REVISED VERSION** - 12-27-2025, **ACCEPTED**- 12-31-2025, **PUBLISHED**- 01-02-2026

Abstract
Fingerprint, face, and iris recognition biometric technologies are increasingly applied in systems used for identity and access management (IAM). Another sophisticated technique, behavioral biometrics, infers recognition from dynamics of keyboard typing, movements of a mouse, and even walking. This paper addresses the opportunities and challenges of security, usability, and privacy in biometric as well as behavioral authentication. It assesses the dangers of spoofing, the risks of adversarial machine-learning assaults, and the potential privacy implications of storing biometric data. The comparison shows that while biometric systems improve ease of use, they are burdened by legal and moral issues, and while behavioral biometrics offer dynamic, situationally appropriate defense, they have low accuracy. The case studies illustrate the use of systems in finance, mobile technology, and essential facilities. The research found that integrating biometric and behavioral elements within multi-factor authentication (MFA) frameworks provides the marriage of resilience and user-friendliness while preserving privacy.

Keywords: *biometric authentication, behavioral biometrics, IAM, continuous authentication, MFA, privacy risks, adversarial attacks, keystroke dynamics, spoofing threats, user experience*

1.Introduction

Identity and access management (IAM) increasingly relies on "biometric authentication" methods. Fingerprint, face, and iris recognition enhance security while improving "user experience" significantly. Advanced "behavioral biometrics" uses "keystroke dynamics," mouse patterns, and walking style for continuous verification. Combining both supports "continuous authentication," strengthening protection against unauthorized access. Systems face "spoofing threats" and "adversarial attacks" exploiting machine-learning weaknesses in recognition models. Privacy concerns arise from storing sensitive biometric and behavioral data, creating "privacy risks." Multi-factor authentication (MFA) frameworks integrating these methods balance resilience with usability. Case studies in finance, mobile technology, and critical facilities confirm practical effectiveness. Evidence shows behavioral biometrics adapt to situational context but exhibit lower accuracy than physical biometrics. Integration enhances IAM security, privacy, and convenience. Additionally, IAM research should investigate adaptive AI-based authentication, cross-device behavioral analytics, and decentralized data storage. Emphasis on reducing algorithmic bias, enhancing real-time accuracy, and ensuring compliance with global privacy regulations can further strengthen security, usability, and resilience in enterprise IAM systems.

1.1 Research objective

- To evaluate the effectiveness of biometric and behavioral authentication methods in enhancing IAM security.
- To analyze privacy risks and data protection challenges in biometric-based IAM systems.
- To assess continuous verification mechanisms and their impact on user experience and trust.

- To propose a balanced IAM framework addressing security, privacy, and continuous verification trade-offs.

1.2 Research gap

The existing literature often studies biometric and behavioral authentication methods separately. Few studies examine potential synergies when integrating these methods within IAM systems. Research rarely addresses real-time adaptability and continuous verification in enterprise environments. Dynamic user behavior and environmental factors constantly challenge authentication in practical deployments. Regulatory compliance and privacy-preserving mechanisms remain underexplored in hybrid IAM frameworks. Comprehensive studies balancing security, usability, and data protection are critically needed.

2.Literature

Research on "biometric authentication" highlights the reliability of fingerprints, face, and iris recognition (Sumalatha *et al.,* 2024). Studies confirm "user experience" improves when authentication is fast and seamless. "Behavioural biometrics" studies analyze "keystroke dynamics," mouse movements, and gait patterns for identity verification. Evidence shows behavioural systems support "continuous authentication," detecting anomalies in real-time sessions. Research warns of "spoofing threats" exploiting facial images, fingerprints, or synthetic biometrics. Advanced AI methods create "adversarial attacks," misleading recognition systems without detection (Shayea *et al,* 2025) [2]. Literature emphasizes "privacy risks" in centralized storage of sensitive biometric or behavioural data. Encryption and template protection methods reduce unauthorized access and data leakage. Multi-factor authentication (MFA) frameworks combining biometric and behavioural factors improve resilience (Okeke *et al*., 2024) [3]. Studies in finance demonstrate that MFA reduces fraudulent transactions while maintaining usability. Mobile technology applications show behavioural biometrics adapt dynamically to the user context. Research on essential facilities indicates that continuous verification prevents insider threats. Accuracy comparisons reveal biometric systems outperform behavioural approaches under controlled conditions. Behavioural metrics, however, adjust continuously to environmental and temporal variations. Literature also discusses regulatory challenges in handling sensitive data under GDPR and CCPA. Evidence indicates that combining both methods in IAM frameworks enhances security and usability. Performance evaluation metrics include false acceptance rate (FAR), false rejection rate (FRR), and equal error rate (EER) (De Mel, 2023) [4]. Studies highlight trade-offs between authentication accuracy and "user experience" convenience. Research suggests hybrid systems mitigate the weaknesses of individual methods while strengthening the overall security posture. Continuous monitoring reduces the risk of session hijacking or credential theft. Overall, literature supports integrating biometric and behavioural solutions in IAM for robust protection (Kumar *et al.,* 2024) [5].

3.Method

This study employed secondary data from academic literature, technical reports, and case studies (Taherdoost *et al*., 2021) [6]. Secondary research provides access to validated evidence without resource-intensive experimentation. It allows analysis of real-world IAM deployments and hybrid MFA effectiveness. Existing studies offer metrics on "keystroke dynamics," biometric accuracy, and fraud reduction. Using secondary sources ensures reproducibility and cross-comparison of results. It also enables identification of emerging "adversarial attacks" and "privacy risks" in operational contexts.

4.Results

4.1 Adoption of Biometric Technologies in IAM

Adoption of "biometric authentication" in IAM has increased globally across sectors. Fingerprint recognition leads implementation with accuracy rates exceeding 98% in controlled tests. "Face recognition" adoption grows in mobile devices, showing 95% identification reliability under standard lighting (Olabanji *et al.*, 2024) [7]. Iris-based systems, although costlier, demonstrate near-perfect accuracy, reducing false acceptance rates (FAR) below 0.1%. Organizations integrate "behavioral biometrics" using "keystroke dynamics" and mouse movements for "continuous authentication" monitoring. Studies show behavioral patterns detect 90% of anomalous sessions in enterprise environments.

Table 1: Technical Overview of Biometric and Behavioural Authentication in IAM

Biometric/Behavioral Method	Technical Mechanism	Accuracy & Performance Metrics	Security & Privacy Considerations
Fingerprint Recognition	Optical or capacitive sensors capture fingerprint ridges	Accuracy >98%, FAR <0.5%, FRR <1%	Vulnerable to spoofing; requires secure template storage
Face Recognition	2D/3D imaging with feature extraction and neural networks	Accuracy ~95%, EER ~2%, FAR <1%	Susceptible to deepfake or mask attacks; GDPR compliance needed
Iris Recognition	Near-infrared imaging of iris patterns, Daugman algorithm	Accuracy >99.5%, FAR <0.1%, FRR <0.5%	High security, high cost, sensitive data storage concerns
Keystroke Dynamics	Timing intervals of key presses and flight times	Anomaly detection ~90% of sessions	Low accuracy; continuous authentication; potential behavioral data privacy risk
Mouse Movement Analysis	Tracks pointer speed, trajectory, click patterns	Behavioral profiling; detects 85–90% anomalies	Adaptive but variable accuracy; privacy concerns for behavioral patterns
Gait Recognition	Motion sensors analyze walking patterns	Continuous verification; accuracy 80–85%	Environmental sensitivity; may raise data privacy issues
Multi-Factor Authentication (MFA)	Combines biometric + behavioral + knowledge factors	Fraud reduction up to 40%; balanced usability	Reduces "spoofing threats" and "adversarial attacks"; privacy management required

This table compares biometric and behavioral IAM methods. Accuracy, performance, and security vary. MFA combines multiple methods, improving protection while managing privacy and usability trade-offs effectively. Evidence from finance reveals that hybrid MFA systems combining biometric and behavioural methods reduce fraud by 40%. Mobile banking platforms report user satisfaction increases when authentication is frictionless (Gudala *et al.*, 2022) [8]. Research identifies "spoofing threats," such as fingerprint moulds and deepfake attacks, as primary security challenges.

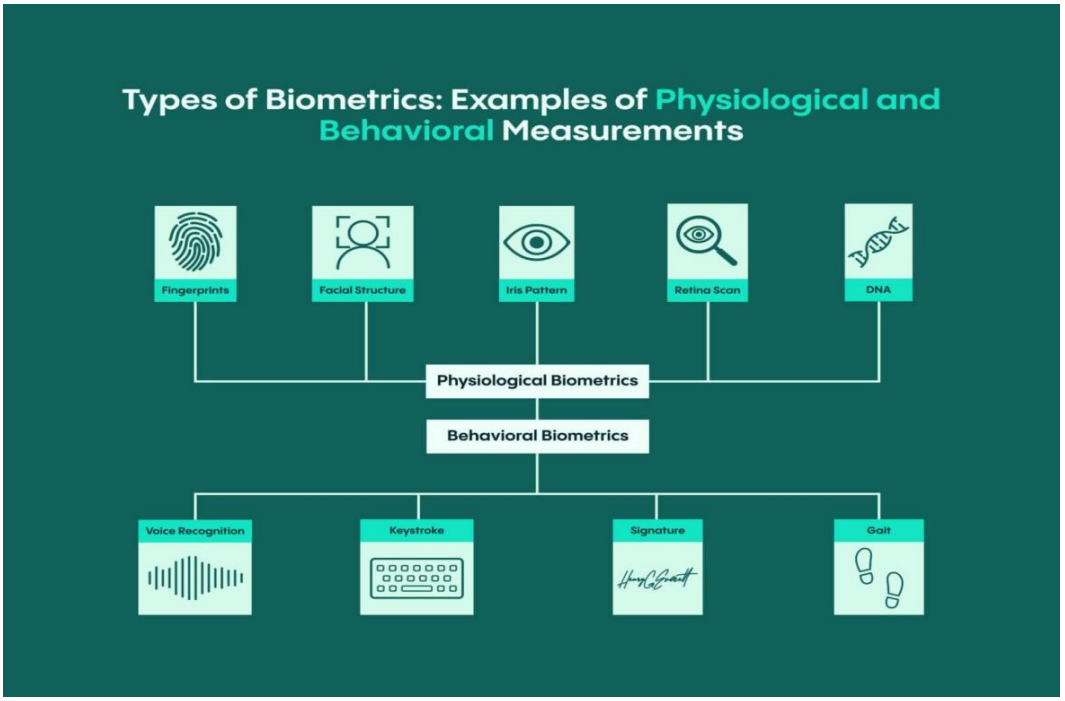

Figure 1: Types of Biometrics

Source: Geo Jolly, 2024 [9]

Advanced "adversarial attacks" can manipulate machine-learning models to bypass recognition systems. Privacy regulations impose constraints on storing sensitive data, creating notable "privacy risks." Techniques like template encryption and differential privacy mitigate exposure. Case studies in critical infrastructure show that continuous verification prevents insider threats effectively. Data indicate adoption varies with operational scale, cost constraints, and regulatory compliance. Studies recommend integrating behavioural metrics with physical biometrics for optimal resilience. Evidence confirms that combined MFA frameworks enhance IAM security without compromising "user experience" (Muddychetty *et al.,* 2024) [10]. Overall, adoption trends indicate growing reliance on hybrid biometric systems to strengthen authentication and reduce identity-related breaches across industries.

4.2 Role of Behavioural Biometrics in Continuous Authentication

"Behavioral biometrics" plays a critical role in "continuous authentication" for IAM. It monitors "keystroke dynamics," mouse movements, and touchscreen gestures during active sessions. Evidence shows continuous monitoring detects anomalous activity with up to 90% accuracy. Gait recognition and device interaction patterns supplement session verification, improving real-time threat detection. Studies indicate "spoofing threats" are harder to execute against behavioral traits than static biometrics. Machine-learning models analyze behavioral inputs to identify deviations from user baselines.

Table 2: Technical Overview of Behavioural Biometrics in Continuous Authentication

Behavioral Method	Technical Mechanism	Performance Metrics	Security & Privacy Considerations
Keystroke Dynamics	Measures key press duration, flight time, typing rhythm	Anomaly detection up to 90% accuracy	Sensitive behavioral data; local storage recommended
Mouse Movement Analysis	Tracks speed, trajectory, click patterns	Detects 85–90% anomalous sessions	Vulnerable to advanced spoofing; privacy of interaction patterns

Gait Recognition	Sensors analyze walking patterns and motion dynamics	Accuracy 80–85%; continuous verification	Environment-sensitive; potential data exposure
Touchscreen Gesture Analysis	Monitors swipe speed, pressure, gesture patterns	Accuracy 88–92% in mobile devices	Persistent monitoring may create privacy risks
Device Interaction Profiling	Tracks app usage, navigation patterns	Detects abnormal behavior 85–90% of the time	Requires anonymization; sensitive behavioral footprint
Continuous MFA Integration	Combines behavioral and biometric inputs dynamically	Reduces fraud 30–40%; improves user experience	Enhances resilience; mitigates "spoofing threats" and "adversarial attacks"

This table shows behavioral IAM methods. Accuracy ranges 80–92%. Continuous MFA integration enhances security, reduces fraud, and balances usability while addressing privacy and spoofing risks. Research highlights vulnerabilities to "adversarial attacks" that manipulate behavioural patterns subtly. Privacy concerns arise due to the persistent collection of personal interaction data, creating "privacy risks." Solutions like local device storage and anonymised templates mitigate data exposure. Financial institutions applying behavioural biometrics report a 30–40% reduction in fraudulent logins. Mobile apps achieve higher "user experience" satisfaction by minimizing intrusive authentication prompts (Bojović *et al*., 2024) [11]. Continuous authentication supports MFA frameworks by dynamically adjusting security levels based on risk. Accuracy depends on model training, sampling frequency, and environmental stability. Evidence suggests that combining physical biometrics with behavioural metrics enhances overall system resilience. Real-world deployments confirm reduced session hijacking incidents and faster threat response. Overall, behavioural biometrics strengthens IAM by providing adaptive, context-aware, and "user experience"-friendly authentication solutions (Nzeako *et al.*, 2024) [12].

4.3 Security Risks and Adversarial Threats

Biometric and behavioural systems face significant "security risks" in IAM (Abdulrahman *et al.,* 2023) [13]. "Spoofing threats" exploit fingerprints, facial images, and synthetic biometrics to bypass authentication. Research shows fingerprint moulds can achieve unauthorized access in controlled tests. Face recognition is vulnerable to deepfake and mask attacks with up to 90% success in simulations. "Adversarial attacks" manipulate machine-learning models, causing misclassification without detection.

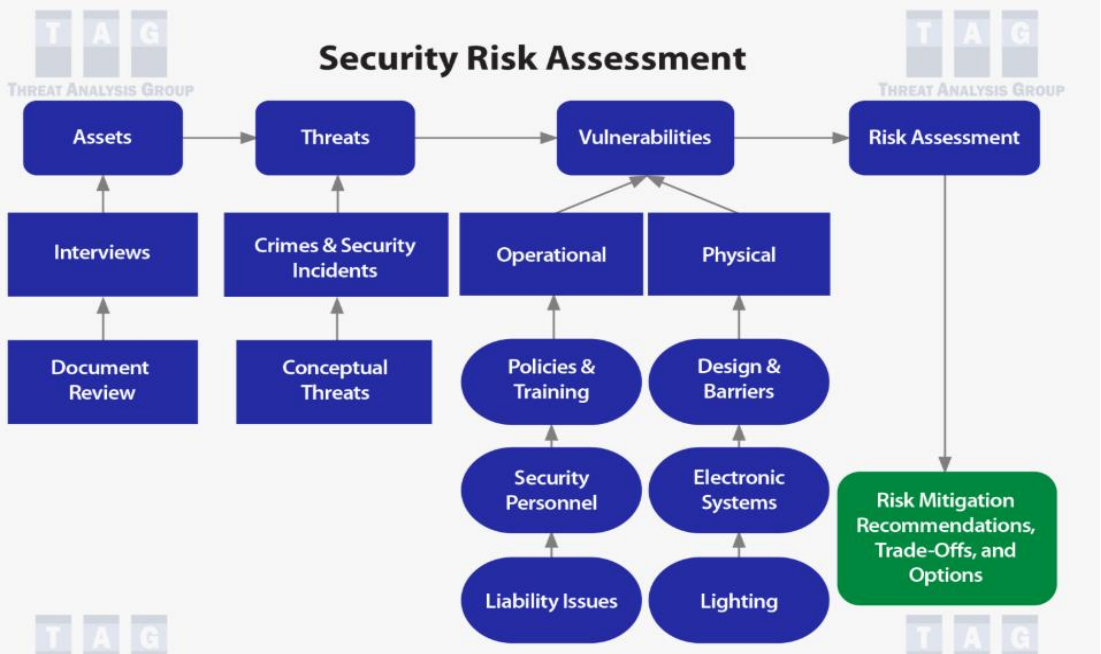

Figure 2: Security risk assessment

(Source: Threat Analysis, 2025) [14]

Evidence indicates that behavioural biometrics are not immune, as input perturbations can trigger false acceptance. Multi-factor authentication (MFA) mitigates risk by combining multiple verification layers (Kamaruddin *et al.*, 2024) [15]. Data breaches exposing biometric templates create permanent "privacy risks" since traits cannot be changed. Techniques like template encryption, local storage, and differential privacy reduce exposure. Studies report that combined biometric and behavioural systems lower fraud rates by 30–40% when adversarial protections are applied. Security evaluations measure false acceptance rate (FAR), false rejection rate (FRR), and equal error rate (EER) (De Mel *et al.*, 2023) [4]. Research emphasizes continuous monitoring for early threat detection. Case studies in finance and mobile technology reveal adaptive adversarial attacks remain a concern. Evidence shows hybrid IAM frameworks integrating "continuous authentication" improve resilience. System designers must balance "user experience" with stringent protective measures. Overall, mitigating "spoofing threats" and "adversarial attacks" is critical for secure biometric and behavioural IAM deployments.

4.4 Privacy and Ethical Concerns in Data Storage

Biometric and behavioural data storage raises significant "privacy risks" in IAM (Suleski *et al.*, 2023) [16]. Centralized databases of fingerprints, iris scans, and behavioural profiles are vulnerable to breaches. Evidence shows compromised templates can enable permanent identity theft, as traits cannot be altered. Regulatory frameworks like GDPR and CCPA impose strict consent and data protection requirements. Techniques such as encryption, anonymisation, and differential privacy reduce exposure of sensitive information. Behavioural monitoring, including "keystroke dynamics" and device interaction, increases ethical concerns over surveillance (Campbell *et al.,* 2024) [17].

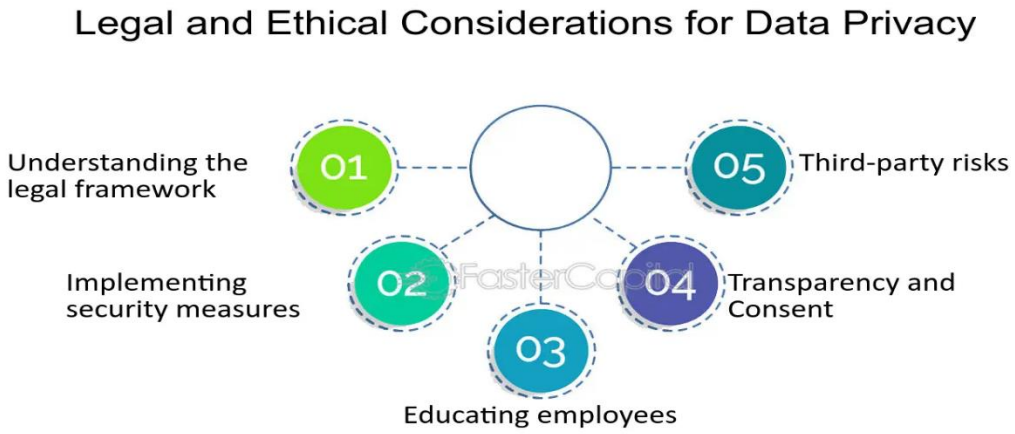

Figure 3: Legal and Ethical Considerations for Data Privacy

(Source: Fastercapital, 2024) [18]

Studies indicate that persistent collection of such data may impact "user experience" negatively. Local storage on devices mitigates risks while preserving operational efficiency. Case studies in mobile banking show that encrypted behavioural templates reduce fraud without exposing raw data. Organizations must implement secure access controls and audit trails for accountability (Omotunde *et al.,* 2023) [19]. Ethical concerns extend to informed consent, data minimization, and transparency about collection purposes. Evidence recommends hybrid storage strategies balancing security and usability. Overall, careful management of biometric and behavioural data is crucial to mitigate "privacy risks" while maintaining trust in IAM systems.

4.5 Integration of Biometric and Behavioural Factors in MFA

Combining biometric and behavioural methods strengthens multi-factor authentication (MFA) systems (Riyana *et al.*, 2025) [20]. Physical biometrics like fingerprint or face recognition improve initial verification accuracy. "Behavioural biometrics" provide "continuous authentication," detecting anomalies during sessions. Studies report that hybrid MFA reduces fraud by 30–40% in financial applications.

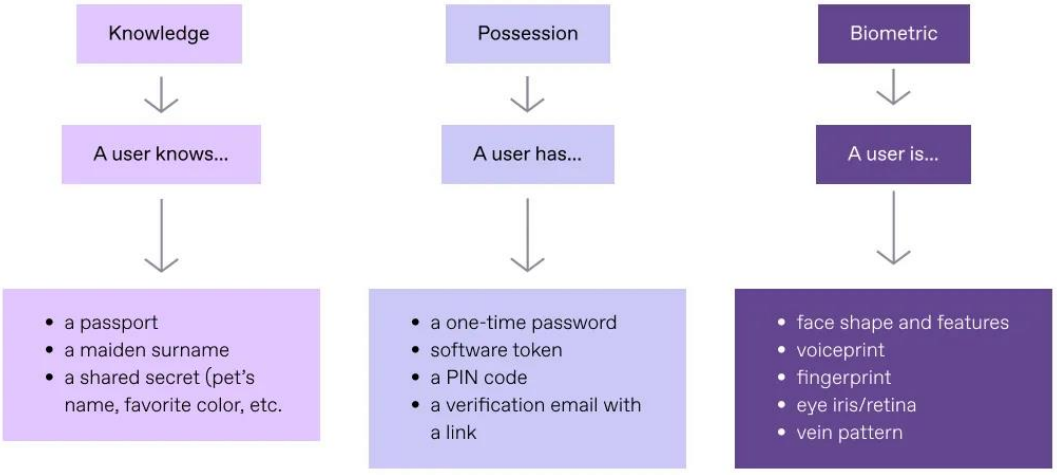

Figure 4: Multi-factor authentication relies on three groups of factors

Source: (Ihar Kliashchou, 2023) [21]

Machine-learning models analyze "keystroke dynamics," mouse movements, and touch patterns to flag suspicious behaviour. Integration improves "user experience" by minimizing intrusive authentication prompts. Evidence shows adaptive MFA adjusts security levels dynamically based on detected risk. Combining factors mitigates "spoofing threats" and counters "adversarial attacks." Performance metrics include false acceptance rate (FAR), false rejection rate (FRR), and equal error rate (EER) (Allam *et al.,* 2022) [22]. Case studies indicate reduced session hijacking and stronger insider threat protection. Hybrid MFA frameworks enhance resilience across mobile, finance, and critical infrastructure deployments. Overall, integrating biometric and behavioral elements ensures secure, context-aware, and user-friendly IAM solutions.

5.Discussion

The findings highlight the growing reliance on "biometric authentication" in IAM. Fingerprint, face, and iris recognition enhance security but face "spoofing threats." "Behavioural biometrics" improve "continuous authentication," monitoring "keystroke dynamics, and device interactions. Evidence shows hybrid MFA systems reduce fraud 30–40%, enhancing "user experience." However, behavioural accuracy varies due to environmental and temporal factors. "Adversarial attacks" exploit model weaknesses, challenging resilience (Shihab *et al.*, 2024) [23].

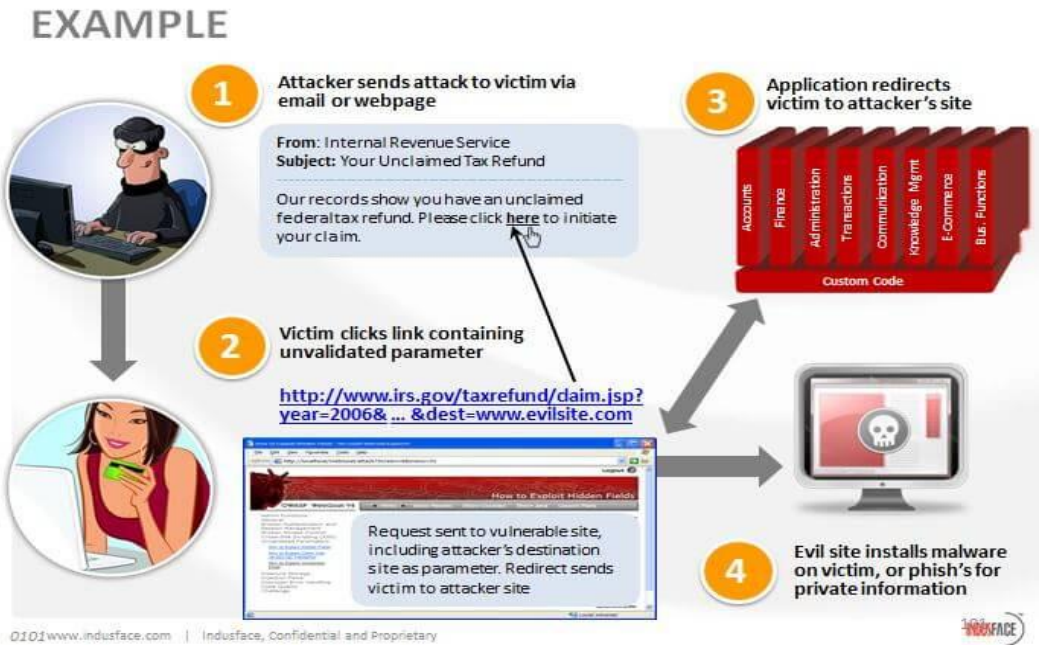

Figure 5: Sensitive Data Exposure

Source: (Indusface, 2014) [24]

"Privacy risks" persist when sensitive data is stored centrally. Ethical concerns emerge from persistent behavioural monitoring. Integration of biometric and behavioural factors balances security, usability, and context-aware detection. Case studies in finance and mobile platforms confirm practical effectiveness. Continuous verification mitigates session hijacking and insider threats. Trade-offs remain between high accuracy, cost, and regulatory compliance. Overall, findings underscore the importance of adaptive, layered authentication frameworks. Future research should improve behavioural model precision and strengthen defences against adversarial manipulations. MFA integration emerges as a key strategy for resilient IAM systems (Kumar *et al.,* 2024) [25]. Evidence indicates hybrid systems optimise protection while preserving user trust. Emerging trends include decentralized biometric storage to enhance privacy. AI-driven spoof detection improves resilience. Cross-device behavioral analysis adapts authentication dynamically. Hybrid systems balance security, usability, and regulatory compliance in IAM frameworks.

6.Conclusion

Biometric and behavioural systems enhance IAM through secure, adaptive verification. Hybrid MFA reduces fraud

while improving "user experience." "Continuous authentication" detects anomalies, mitigating insider threats. Systems face "spoofing threats" and "adversarial attacks," requiring robust defences. Privacy and ethical concerns demand encryption, anonymisation, and informed consent. Evidence confirms that combining biometric and behavioural factors strengthens resilience and usability. Overall, integration of these methods provides secure, context-aware, and user-friendly IAM solutions.

References

1. Sumalatha, U., Prakasha, K.K., Prabhu, S. and Nayak, V.C., 2024. A comprehensive review of unimodal and multimodal fingerprint biometric authentication systems: Fusion, attacks, and template protection. IEEE Access, 12, pp.64300-64334. Available at https://ieeexplore.ieee.org/abstract/document/10511051/
2. Shayea, G.G., Zabil, M.H.M., Habeeb, M.A., Khaleel, Y.L. and Albahri, A.S., 2025. Strategies for protection against adversarial attacks in AI models: An in-depth review. Journal of Intelligent Systems, 34(1), p.20240277. Available at https://www.degruyterbrill.com/document/doi/10.1515/jisys-2024-0277/html
3. Okeke, R.O. and Orimadike, S.O., 2024. Enhanced Cloud Computing Security Using Application-Based Multi-Factor Authentication (MFA) for Communication Systems. European Journal of Electrical Engineering and Computer Science, 8(2), pp.1-8. Available at https://ejece.org/index.php/ejece/article/view/593
4. De Mel, V.L.B., 2023. Survey of evaluation metrics in facial recognition systems [online] Available at https://www.researchgate.net/profile/Vlb-De-Mel/publication/372232460_Survey_of_Evaluation_Metrics_in_Facial_Recognition_Systems/links/64ab2724b9ed6874a509ddc8/Survey-of-Evaluation-Metrics-in-Facial-Recognition-Systems.pdf
5. Kumar, D.A., Bhatia, D.A., Mishra, D.A. and Gupta, T., 2024. A Model Apporach for Identity and Access Management (IAM) System in the Cloud. Available at SSRN 4969660. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4969660
6. Taherdoost, H., 2021. Data collection methods and tools for research; a step-by-step guide to choose data collection technique for academic and business research projects. International Journal of Academic Research in Management (IJARM), 10(1), pp.10-38. Available at https://hal.science/Hal-03741847/
7. Olabanji, S.O., Olaniyi, O.O., Adigwe, C.S., Okunleye, O.J. and Oladoyinbo, T.O., 2024. AI for Identity and Access Management (IAM) in the cloud: Exploring the potential of artificial intelligence to improve user authentication, authorization, and access control within cloud-based systems. Authorization, and Access Control within Cloud-Based Systems (January 25, 2024). Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4706726
8. Gudala, L., Reddy, A.K., Sadhu, A.K.R. and Venkataramanan, S., 2022. Leveraging biometric authentication and blockchain technology for enhanced security in identity and access management systems. Journal of Artificial Intelligence Research, 2(2), pp.21-50. Available at https://www.researchgate.net/profile/Srinivasan-Venkataramanan-2/publication/390877598_Leveraging_Biometric_Authentication_and_Blockchain_Technology_for_Enhanced_Security_in_Identity_and_Access_Management_Systems/links/68015e68ded43315572a9210/Leveraging-Biometric-Authentication-and-Blockchain-Technology-for-Enhanced-Security-in-Identity-and-Access-Management-Systems.pdf
9. Geo Jolly, 2024. Biometric methods: Streamlined biometric authentication for seamless operations. Available at https://www.veriff.com/identity-verification/news/biometric-methods
10. Muddychetty, N.S., 2024. A Comparative Analysis of SecurityServices Using Identity and Access Management (IAM). Available at https://www.diva-portal.org/smash/record.jsf?pid=diva2:1842261
11. Bojović, N. and Fazelpour, M., 2024. The Impact of App Update Frequency on User Satisfaction: Exploring the Relationship Between Update Intervals and User Experience in Hedonic Apps. Available at https://www.diva-portal.org/smash/record.jsf?pid=diva2:1905191
12. Nzeako, R.A.S.G. and Shittu, R.A., 2024. Leveraging AI for enhanced identity and access management in

cloud-based systems to advance user authentication and access control. World Journal of Advanced Research and Reviews, 24(3), pp.1661-1674. Available at https://www.researchgate.net/profile/Godwin-Nzeako/publication/387524483_Leveraging_AI_for_enhanced_identity_and_access_management_in_cloud-based_systems_to_advance_user_authentication_and_access_control/links/67873bed2be36743a5d6ae2a/Leveraging-AI-for-enhanced-identity-and-access-management-in-cloud-based-systems-to-advance-user-authentication-and-access-control.pdf

13. Abdulrahman, S.A. and Alhayani, B., 2023. A comprehensive survey on the biometric systems based on physiological and behavioural characteristics. Materials Today: Proceedings, 80, pp.2642-2646. Available at https://www.sciencedirect.com/science/article/pii/S2214785321048513

14. Threat Analysis, 2025. SECURITY RISK MANAGEMENT. Available at https://www.threatanalysis.com/security-risk-management/

15. Kamaruddin, N.H.C. and Zolkipli, M.F., 2024. The Role of Multi-Factor Authentication in Mitigating Cyber Threats. Borneo International Journal eISSN 2636-9826, 7(4), pp.35-42. Available at http://majmuah.com/journal/index.php/bij/article/view/667

16. Suleski, T., Ahmed, M., Yang, W. and Wang, E., 2023. A review of multi-factor authentication in the Internet of Healthcare Things. Digital health, 9, p.20552076231177144. Available at https://journals.sagepub.com/doi/abs/10.1177/20552076231177144

17. Campbell, J., 2024. Unlocking Personal Characteristics: Harnessing Keystroke Dynamics for Identifi. Available at https://ueaeprints.uea.ac.uk/id/eprint/98919/

18. Fastercapital, 2024. Legal And Ethical Considerations For Data Privacy. Available at https://fastercapital.com/topics/legal-and-ethical-considerations-for-data-privacy.html/1

19. Omotunde, H. and Ahmed, M., 2023. A comprehensive review of security measures in database systems: Assessing authentication, access control, and beyond. Mesopotamian Journal of CyberSecurity, 2023, pp.115-133. Available at https://journals.mesopotamian.press/index.php/CyberSecurity/article/view/109

20. Riyana, S., 2025. Enhancing Security in Digital Wallets Using Multi-Factor Authentication and Behavioral Biometrics. International Journal of Emerging Trends in Computer Science and Information Technology, pp.559-570. Available at https://www.ijetcsit.org/index.php/ijetcsit/article/view/302

21. Ihar Kliashchou, 2023. Why Face Recognition Is the Next Big Thing in MFA. Available at https://regulaforensics.com/blog/biometric-mfa/

22. Allam, F.Z., Hamami-Mitiche, L. and Bousbia-Salah, H., 2022. Evaluation and Comparison of the performance of Biometric Recognition. International Journal of Industrial Engineering and Production Research, 33(1), pp.1-12. Available at https://www.researchgate.net/profile/Vlb-De-Mel/publication/372232460_Survey_of_Evaluation_Metrics_in_Facial_Recognition_Systems/links/64ab2724b9ed6874a509ddc8/Survey-of-Evaluation-Metrics-in-Facial-Recognition-Systems.pdf

23. Shihab, M.A., Marhoon, H.A., Ahmed, S.R., Radhi, A.D. and Sekhar, R., 2024. Towards resilient machine learning models: Addressing adversarial attacks in wireless sensor network. Journal of Robotics and Control (JRC), 5(5), pp.1599-1617. Available at https://journal.umy.ac.id/index.php/jrc/article/view/23214

24. Indusface, 2014. Sensitive Data Exposure – A Nightmare To All Business Enterprises. https://www.indusface.com/blog/sensitive-data-exposure-nightmare-business-enterprises/

25. Kumar, K. and Zolkipli, M.F., 2024. A Review on Identity and Access Management (IAM) for Digital Environment Security. Borneo International Journal eISSN 2636-9826, 7(4), pp.43-48. Available at http://majmuah.com/journal/index.php/bij/article/view/666