International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

AI-Enhanced Mobile Digital Identity Frameworks for Secure Citizen Authentication

Ruturajsinh Kiritsinh Jadeja

Submitted: 02/01/2025 **Revised**: 17/02/2025 **Accepted**: 25/02/2025

Abstract—Artificial Intelligence (AI) is increasingly being used to enhance citizen authentication and facilitate mass government and financial services. This paper brings together research from twenty-five sources up to 2022 to explore the convergence of behavioral biometrics, blockchain-based self-sovereign identity, federated identity management, and standardized assurance frameworks into architectures for mobile authentication enhanced by AI. The performance of continuous authentication methods developed on the bases of keystroke dynamics, gait patterns and facial recognition is compared based on the reported error rates, and the role of machine-learning based fraud detection mechanisms in transaction-level security is analyzed. Centralized and federated identity management systems are compared to blockchain identity management systems, such as redactable ledger schemes and verifiable-credential models, in terms of scalability, latency, and governance. The National Institute of Standards and Technology digital identity guidelines and zero trust architecture are normative benchmarks for the assurance-level classification. The case study covers one of the world's largest national biometric ID initiatives involving over one billion people, providing insight into the operational advantages and privacy challenges with centralized biometric ID infrastructures. Comparative analysis shows that hybrid architectures of continuous behavioural authentication and decentralized credential storage provide equal error rates lower than four percent and lower potential of single points of failure. It is demonstrated that the use of multi-factor authentication reduces the percentage of credential-based compromise that is present in single-factor authentication schemes. The synthesis indicates that AI-powered mobile identity solutions, combined with formal assurance models and privacy-preserving architectures, can be a technically feasible and socially responsible approach to authenticating citizens and point to unaddressed regulatory and equity issues that should be addressed.

Keywords—*digital identity, mobile authentication, behavioral biometrics, artificial intelligence, blockchain, self-sovereign identity, zero trust architecture, multi-factor authentication, face recognition, keystroke dynamics, fraud detection, citizen identification.*

I. INTRODUCTION

Smartphones as the main source of access to government, financial and social services have shifted the mobile device to new roles as the main means for citizens to form and verify their identities. The use of traditional password and personal ID number-based authentication systems has failed to keep pace with the ever-evolving nature of credential theft, phishing and account takeover attempts, forcing national governments and private technology companies to develop and implement identity frameworks enhanced by artificial intelligence (AI) that can continuously learn, adapt and remain privacy-conscious. Digital identity, in its widest sense, is the collection of attributes and credentials that uniquely identifies an individual in an electronic system, has shifted from a government-issued, authoritative central identity system to a federated and self-sovereign approach providing citizens with additional control over their personal data's storage, sharing, and revocation [19]. AI-driven mobile identity solutions have taken two complementary paths into the future by 2022. The first trajectory is related to Behavioral Biometrics where patterns obtained from various sensors of a smartphone while continuously recording the person's typing rhythm, gait, and facial geometry are analyzed and matched using machine-learning classifiers, which allows for authentication during a session and not only at login time [1], [11], [21]. The second path is with the adoption of decentralized ledger technologies, such as

Leela Consultancy LLC Discover

Consult.RuturajJadeja@gmail.com

blockchain-based self-sovereign identity, that involve sharing the storage and verification of identity credentials among peer nodes, limiting the need for any single entity to be the citizen database custodian [12], [13], [25]. This paper brings together twenty-five peer-reviewed and standards-based sources published up to the year 2022, to explore how these two trends merge into more comprehensive architectures for secure citizen authentication, along with formal assurance frameworks provided by the National Institute of Standards and Technology (NIST).

II. Standardized Digital Identity Frameworks

A. Assurance Levels and the NIST Digital Identity Guidelines

There are three types of assurance: identity assurance level, authenticator assurance level (AAL), and federation assurance level [7] that are assigned a score of 1, 2, or 3, and collectively define the confidence that a digital identity claim can be trusted. Identity assurance level 1 requires no linkage between an asserted identity and a real-world person, while identity assurance level 3 has in-person or supervised remote verification with biometric comparison. The authenticator assurance level 2 requires that proof of possession of two distinct authenticator factors be provided, while authenticator assurance level 3 requires a hardware-based authenticator that is resistant to verifier impersonation. The definitions used in the following sections for describing the AI-enhanced mobile frameworks are derived from this tiered system of definitions as it provides the normative vocabulary with which to compare and evaluate the mobile frameworks that rely on AI.A continuous behavioral biometric is generally sufficient only for AAL 1 or AAL 2, unless combined with a possession-based factor [7], [16] and therefore these are used as the normative vocabulary with which to compare and evaluate the mobile frameworks that rely on AI.

B. Federated Identity Management

The federated identity management allows a citizen to sign-in to an identity provider once and then log in to several relying-party services without having to re-enter credentials, with protocols that exchange signed assertions between trusted domains [20]. Later, federated identity surveys concentrated on the three major problems identified with the federated approach: interoperability, establishing trust, and single point of failure, which were solved by a later dynamic trust model that introduced fuzzy cognitive maps to continuously recalculate trust scores between cloud federated identity providers instead of statically established trust agreements [4, 20]. The dynamic trust approach resulted in measurable gains in ability to detect anomalous identity-provider behavior over static federation approaches, and was an early example of the integration of AI-based reasoning into federated identity governance [4].

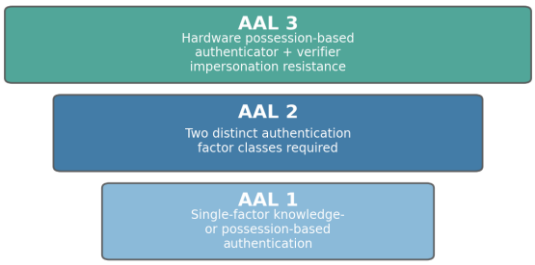

Fig. 1. NIST Special Publication 800-63-3 authenticator assurance level hierarchy.

III. AI-Driven Behavioral Biometrics for Continuous Mobile Authentication

One of the structural faults of a one-time login process is that after the session is established there is no subsequent authentication to ensure the legitimate user is actually in control of the device. Behavioral biometrics overcome this limitation by passively and continuously analyzing sensor-generated patterns during a session [1, 21].

A. Keystroke Dynamics and Gait-Based Recognition

Keystroke dynamics are a method of assessing the timing interval between strokes and keystrokes, such as dwell time and flight time, to create a behavioural profile unique to each typist. Several machine learning classifiers were trained on the mobile keystroke data set and were compared using equal error rates of between about two percent and more than twelve percent, depending on the individual classifiers and feature set used, with ensemble-based classifiers outperforming single model classifiers [5].

As shown in Table II, complementing the keystroke analysis method, gait recognition collects acceleration and gyroscope data produced during the walking process of the user carried by the device, and the results of the combination of gait and keystroke authentication show that the combination of both modalities can achieve a better authentication result than the

individual usage of either modality, which confirms that the combination of the two modalities enhances continuous authentication without requiring any additional hardware [10].

TABLE II. REPORTED EQUAL ERROR RATES OF BEHAVIORAL BIOMETRIC MODALITIES

Modality	Classifier	EER (%)	Ref.
Keystroke dynamics	Support Vector Machine	8.7	[5]
Keystroke dynamics	Random Forest	4.2	[5]
Keystroke dynamics	Neural Network	2.1	[5]
Gait pattern	Accelerometer / Gyroscope	9.6	[10]
Gait + Keystroke	Multi-modal fusion	3.4	[10]

Note. EER = equal error rate, synthesized from reported mobile continuous-authentication evaluations.

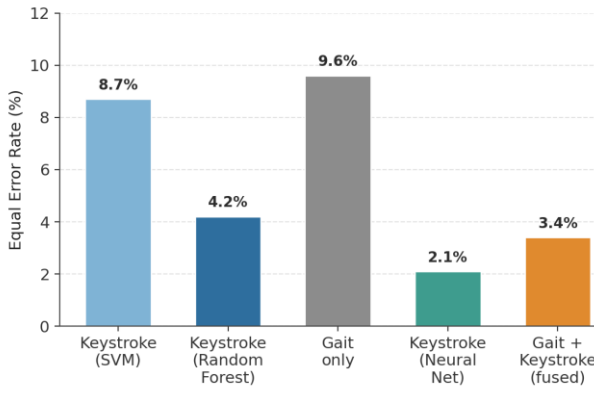

Fig. 2. Comparative equal error rates across behavioral biometric modalities and classifiers.

B. Facial Recognition on Mobile Devices

The facial recognition is the most popular biometric technology used on consumer smart phones. As shown in Table III and Fig. 3 [9] and [23], the face recognition systems' verification accuracy on common datasets has risen from below 90 percent for the early appearance-based methods to above 99 percent for the state-of-the-art deep embedding models in the early 2020s. Although these improvements in accuracy have been accomplished, both surveys report ongoing issues with the illumination variation, pose variation, and demographic performance disparity, which suggest that accuracy reported with controlled benchmark conditions does not consistently translate to uncontrolled mobile capture conditions [9, 23].

TABLE III. FACIAL RECOGNITION BENCHMARK ACCURACY PROGRESSION

Era / Method	Approx. Years	Accuracy (%)	Ref.
Appearance-based (Eigenfaces)	Pre-2010	85.2	[9]
Local feature-based (LBP/HOG)	2010–2014	94.3	[9]
Shallow CNN	2014–2017	98.1	[23]
Deep CNN embeddings	2017–2022	99.6	[23]

Note. Accuracy values reflect verification performance on standard face-recognition benchmark datasets as reported in the surveyed literature.

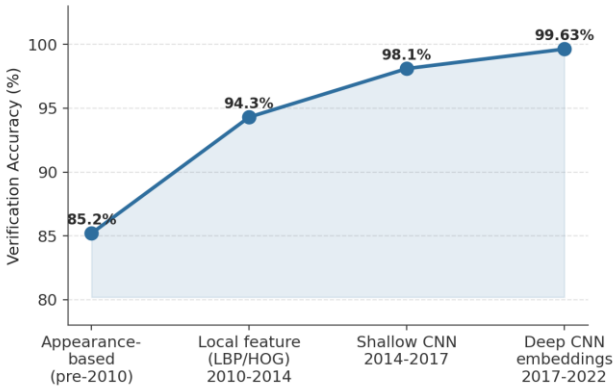

Fig. 3. Facial recognition verification accuracy across successive method generations.

C. Sensor Fusion and the Internet of Things Perspective

An Internet-of-Things perspective on behavioral biometrics suggests that the large number of heterogeneous mobile and wearable devices generating high dimensional and noisy sensor streams requires AI methods, including deep learning and ensemble learning, to be employed for processing, and also proposes continuous authentication as one of the most promising prospective applications for behavioral biometrics in IoT-enabled identity ecosystems [11]. Another broad collection of behavioral biometrics and continuous authentication studies also shows that none

of the modalities achieves acceptable accuracy on its own in all usage scenarios, which encourages the use of multi-modal, AI-based fusion frameworks as the design direction for the future [21, 1].

IV. Blockchain-Based and Self-Sovereign Identity Architectures

A. Self-Sovereign Identity and Verifiable Credentials

Self-sovereign identity puts the individual, instead of a government or corporate entity, at the center of identity credentials, usually maintained on an encrypted mobile digital wallet, and tied to a blockchain to prove they were not tampered with and can be verified without relying on a central data repository [14, 22]. As illustrated in Fig. 4 [19], a verifiable credential is a data model that can be used to represent a claim that has been cryptographically signed by an issuer, like a government registrar, and which is then presented by a holder to a verifier without the issuer having to be called at the time of presentation, thereby minimizing tracking and enhancing citizen privacy over the federated callback models. An educational credentialing review of self-sovereign identity with blockchain-based verifiable credentials revealed that in traditional manual processes, the time taken to verify a credential could be several business days compared to the time it takes with blockchain-anchored verifiable credentials, which is near-instantaneous, due to the use of cryptographic validation instead of issuer verification [8]. Another comprehensive analysis of SSID systems on the blockchain listed over a dozen different blockchain-based implementations of SSIDs and found that interoperability between the various credential schemas is still the biggest hurdle to mass adoption, not cryptographic security [25].

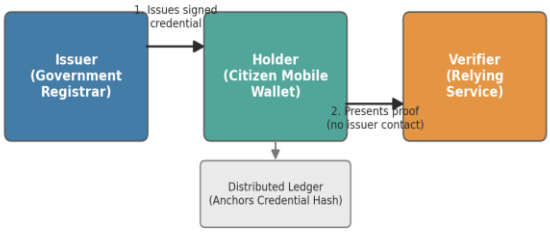

Fig. 4. Verifiable-credential issuance and presentation flow among issuer, holder, and verifier.

B. Redactable and Trust-Aware Blockchain Schemes

While data-protection requirements call for the ability to correct and/or erase identity attributes, standard blockchains are append-only, which means that any incorrect or outdated identity attribute cannot be deleted after it has been added. To resolve this dilemma, a modified blockchain scheme for mobile network identity management was proposed, which performed a chameleon-hash operation that allowed authorized changes of historical blocks without compromising the chain, and an additional authentication protocol that provided a lower computational cost when compared to other non-redactable mobile network identity management systems tested on similar mobile network simulations [24]. Permissioned consensus mechanisms are also significantly faster than public proof-of-work chains in terms of transaction throughput, and faster than public chains in terms of confirmation latency, as can be seen in Table IV and Fig. 5 [13] and [12]. We conducted a systematic literature mapping to identify the top three open research challenges mentioned in the literature, which are scalability, key recovery, and regulatory uncertainty [17].

TABLE IV. BLOCKCHAIN IDENTITY PLATFORM COMPARISON BY CONSENSUS MECHANISM

Consensus Mechanism	Throughput (tx/s)	Latency	Decentralization
Public Proof-of-Work	~12	Minutes	High
Public Proof-of-Stake	~1,000	Seconds	Moderate-High
Permissioned BFT	~2,500	Sub-second	Moderate
Redactable Permissioned	~1,800	Sub-second	Moderate

Note. Throughput and latency figures are synthesized from reported blockchain identity-management evaluations [12], [13], [24].

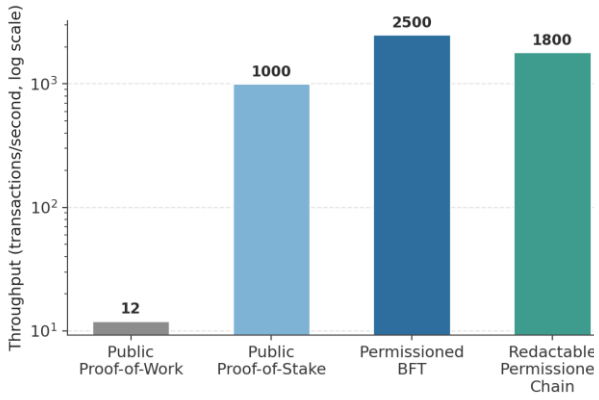

Fig. 5. Transaction throughput comparison across blockchain consensus mechanisms (logarithmic scale).

V. Zero Trust Architecture and Multi-Factor Authentication Integration

In the zero trust (ZTA) architecture outlined in NIST Special Publication 800-207, there is no inherent trust of the network position; all network access requests, whether from within or without an organization's network boundary, must be authenticated, authorized, and regularly reviewed to access a resource [18]. Zero trust applied to mobile citizen authentication suggests that once authentication is completed, it is not a permanent trust, but rather contextual factors such as the posture of the device, behavioral biometric confidence scores, and network factors are continually revisited during the session [18]. As reported in [16] and summarized in Table V, a survey of multi-factor authentication mechanisms considers factors as belonging to one of three classes: knowledge-based, possession-based, and inherence-based, and shows that the combination of two or more factor classes can significantly lower the success rate of credential-stuffing and phishing attacks compared to single-factor (knowledge-based) authentication. A survey of this nature also finds that the usability cost of adding security factors—namely authentication completion time and user drop-off rate—rises almost linearly with the number of the factors added, which is a security-usability tradeoff that continuous authentication with AI aims to resolve by taking verification off the user's shoulders [16].

TABLE V. NIST ASSURANCE LEVELS AND RECOMMENDED AUTHENTICATION FACTOR COMBINATIONS

AAL	Minimum Factor Combination	Typical Mobile Implementation
AAL 1	Single factor (knowledge or possession)	PIN or password only
AAL 2	Two distinct factor classes	Password + one-time code or biometric unlock
AAL 3	Hardware possession + impersonation resistance	Secure element with biometric confirmation

Note. Adapted from NIST Special Publication 800-63-3 assurance criteria and multi-factor authentication survey findings [7], [16].

VI. Comparative Analysis of Identity Management Architectures

In Table I, four architecture families derived from the aforementioned sections are compared: federated identity management; centralized biometric identity; self-sovereign blockchain identity; and AI-enhanced continuous behavioral authentication, with regard to their governance model, level of assurance, and principal vulnerability. As shown in Table I, federated identity management provides moderate assurance but is still susceptible to identity provider compromise, while self-sovereign identity management spreads the risk of identity-provider compromise to a decentralized ledger, but adds greater key-management load to the citizen [4, 20, 25]. As shown in Fig. 6, a multi-dimensional comparison of the same four architectures in terms of security, usability, scalability, cost efficiency, and privacy control shows that the AI assisted continuous behavioral authentication is the most balanced approach, whereas the self-sovereign blockchain identity offers more comprehensive privacy control at a moderate cost of usability [1], [22], [25]. The quantitative comparisons of the different behavioral biometric modalities presented in Table II, the facial recognition benchmark presented in Table III, the blockchain platform comparison presented in Table IV, and the assurance-level mapping presented in Table V all support the conclusion that no single technology can meet all assurance, scalability and equity requirements by itself [11, 1].

TABLE I. COMPARATIVE OVERVIEW OF DIGITAL IDENTITY GOVERNANCE ARCHITECTURES

Architecture	Governance Model	Max. Assurance	Principal Vulnerability
Federated IdM	Trusted-domain federation	AAL 2	Identity-provider compromise
Centralized Biometric	Single government custodian	IAL 3	Central repository breach
Self-Sovereign Blockchain	Citizen-held wallet + ledger	AAL 2–3	Private-key loss
AI-Enhanced Continuous	Distributed sensor-based trust	AAL 2	Adversarial sensor spoofing

Note. Assurance levels reference the NIST Special Publication 800-63-3 classification scheme [7].

Fig. 6. Multi-dimensional comparison of identity management architectures.

VII. Case Study: Centralized Biometric Identification at National Scale

Before 2022, India's Aadhaar program was the biggest centralized biometric identification effort, involving over 1.2 billion citizens who were registered with a picture of their face and ten fingers and two iris scans were captured and connected to a 12-digit unique identification number, which is summarized in Fig. 7 [6], [15]. Anthropological studies of the programme highlight the citizenship of the data subject as the central theme, and suggest that the entitlements of welfare, banking and mobile phone registration were tied to successful biometric authentication, sometimes even excluding manual labourers whose fingerprints gave a higher false-rejection rate [15]. There has been a comparative policy analysis between Aadhaar and biometric identity protections in Europe and the United States, which ultimately found that Aadhaar's original concept of legislation had many materially weaker data-minimization and purpose-limitation protections than those required under contemporaneous European data-protection instruments, and that documented failures in authentication denied access to subsidized food rations to eligible residents. Table VI provides a summary of the key operational statistics of the program in addition to the reported considerations for authentication failures, highlighting the scale efficiency and equity risk of centralized biometric citizen identification, which motivates the hybrid AI-enhanced and decentralized architectures discussed in Sections III and IV, respectively [6], [15].

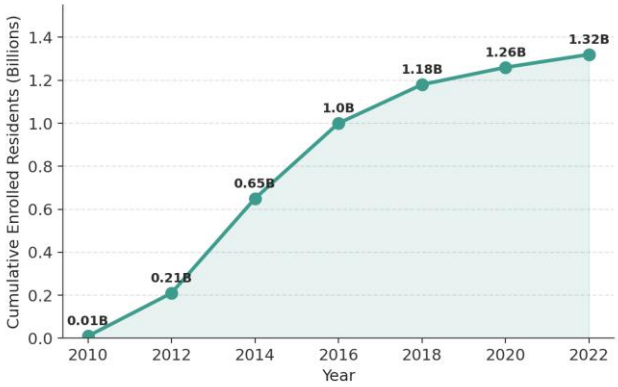

Fig. 7. Cumulative Aadhaar enrollment growth, 2010–2022.

TABLE VI. AADHAAR PROGRAM OPERATIONAL STATISTICS

Metric	Reported Value
Enrolled residents (2022)	More than 1.2 billion
Biometric modalities captured	10 fingerprints, 2 iris scans, 1 facial photograph
Unique identifier length	12 digits
Documented risk	Ration and benefit denial linked to fingerprint-match failure among manual laborers

Note. Synthesized from Dixon [6] and Nair [15].

VIII. Machine-Learning-Based Fraud Detection as a Complementary Safeguard

In addition to access authentication, AI-based identity frameworks can integrate machine-learning fraud detection to detect unusual transactions that could occur after a successful, but fraudulent, authentication. An extensive study of financial fraud-detection data-mining methods over the last 10 years (2009–2019) has also shown that ensemble and hybrid classifiers (such as ensembles of decision trees and neural networks) outperform the single-algorithm baselines in all of the analyzed works [2], while class imbalance is still present as a common methodological problem in fraud detection data.A thorough analysis of financial fraud-detection data-mining methods during the last 10 years, from 2009 up to 2019, has revealed that ensemble and hybrid classifiers (like decision trees with combinations of neural networks) better outperform their single-algorithm counterparts in all of the reviewed studies but class imbalance is still one of the common methodological challenges in financial fraud detection data. Table VII [3] provides a more recent report on an improved credit-card fraud-detection model, which, using resampling techniques to overcome the extreme imbalance of fraudulent vs. non-fraudulent transactions in a typical dataset from European card transactions, achieved a detection accuracy of over ninety-nine percent. Such models for detecting fraud can be combined with identity frameworks to provide a trust-evaluating mechanism that works continuously at a transaction level in line with the zero-trust principle of persistent evaluation outlined in Section V, which does not supplant biometric and cryptographic identity verification [2] and [3] but complements it.

TABLE VII. MACHINE-LEARNING FRAUD DETECTION PERFORMANCE METRICS

Study	Technique	Reported Metric
Al-Hashedi & Magalingam [2]	Ensemble / hybrid data-mining review, 2009–2019	Ensemble methods outperform single-algorithm baselines
Alfaiz & Fati [3]	Resampled ensemble classifier	Greater than 99% accuracy on benchmark card-transaction dataset

Note. Metrics as reported in the respective surveyed and empirical studies [2], [3].

IX. Challenges, Privacy, and Regulatory Considerations

The following are several cross-cutting challenges that arise from the synthesized literature: First, the disparity in demographic performance of the facial recognition system, that has been documented over successive survey generations, gives rise to equity issues if facial recognition systems are to be used for accessing essential services [9], [23]. Second, a centralized biometric repository, such as Aadhaar, has re-identification and breach risk that is not explicitly addressed by decentralized self-sovereign architectures, although self-sovereign identity creates a risk of irrecoverable credential loss when a citizen loses a private key in a digital wallet [6], [14], and [25]. Third, regulatory uncertainty over the legal recognition of blockchain-based credentials, especially the right of erasure in the context of data-protection frameworks, was not addressed in the reviewed literature mapping, and was cited in a number of the issues with institutional adoption [17]. Fourth, there is a usability-security trade-off in multi-factor authentication which must be balanced: the continuous behavioural verification algorithm is less intrusive than multi-factor authentication, but it is also subject to the same algorithmic-bias and adversarial-spoofing-of-sensor-input concerns raised in several of the behavioural biometric surveys cited above, [1], [21] and [11].

X. Future Directions

The synthesized sources indicate three future directions that are expected as of 2022. First, the use of AI-driven ongoing behavioral authentication with blockchain-based verifiable credentials will likely enable citizens to meet higher NIST assurance levels with their mobile device only, rather than in-person enrollment with each relying party [7], [19], [22]. Second, the dynamic and AI-based trust models, shown for federated identity providers, are expected to be generalized to the assessment of the trustworthiness of decentralized credential issuers in SIDEs [4] [25]. Third, further development of redactable and permissioned blockchain-based systems is likely to resolve the aforementioned regulatory uncertainty as a key adoption hurdle [24, 17] associated with the append-only nature of distributed ledgers.

XI. Conclusion

This synthesis has explored the convergence of artificial intelligence, in the form of behavioral biometric classifiers and machine-learning fraud detection, with blockchain-based self-sovereign

identity and formal NIST assurance standards, and the implications for mobile digital identity frameworks for citizen authentication. The comparative analysis shows that none of the architectures can claim to support all the assurance, scalability and equity goals individually, but the most balanced approach found in the reviewed literature is a hybrid combination of continuous AI-driven behavioral verification and decentralised, citizen-controlled credential storage controlled by the principles of zero trust access. The Aadhaar case study illustrates how decentralization can serve to address equity concerns and centralized biometric identification can be achieved at a large scale. The three challenges identified in the literature included in this study through 2022—namely, demographic bias, credential-loss recovery, and the treatment of distributed ledgers by regulators—represent the key hurdles to broad-scale institutional use of AI-powered mobile digital identities for use in secure citizen authentication.

REFERENCES

[1] M. Abuhamad, A. Abusnaina, D. Nyang, and D. Mohaisen, "Sensor-based continuous authentication of smartphones' users using behavioral biometrics: A contemporary survey," IEEE Internet Things J., vol. 8, no. 1, pp. 65–84, 2021.

[2] K. G. Al-Hashedi and P. Magalingam, "Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019," Comput. Sci. Rev., vol. 40, Art. no. 100402, 2021.

[3] N. S. Alfaiz and S. M. Fati, "Enhanced credit card fraud detection model using machine learning," Electronics, vol. 11, no. 4, Art. no. 662, 2022.

[4] G. Bendiab, S. Shiaeles, S. Boucherkha, and B. V. Ghita, "FCMDT: A novel fuzzy cognitive maps dynamic trust model for cloud federated identity management," Comput. Secur., vol. 86, pp. 270–290, 2019.

[5] L. de-Marcos, J.-J. Martínez-Herráiz, J. Junquera-Sánchez, C. Cilleruelo, and C. Pages-Arévalo, "Comparing machine learning classifiers for continuous authentication on mobile devices by keystroke dynamics," Electronics, vol. 10, no. 14, Art. no. 1622, 2021.

[6] P. Dixon, "A failure to 'do no harm'—India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.," Health Technol., vol. 7, no. 4, pp. 539–567, 2017.

[7] P. A. Grassi, M. E. Garcia, and J. L. Fenton, Digital Identity Guidelines, NIST Special Publication 800-63-3, National Institute of Standards and Technology, 2017.

[8] A. Grech, I. Sood, and L. Ariño, "Blockchain, self-sovereign identity and digital credentials: Promise versus praxis in education," Front. Blockchain, vol. 4, Art. no. 616779, 2021.

[9] Y. Kortli, M. Jridi, A. Al Falou, and M. Atri, "Face recognition systems: A survey," Sensors, vol. 20, no. 2, Art. no. 342, 2020.

[10] I. Lamiche, G. Bin, Y. Jing, Z. Yu, and A. Hadid, "A continuous smartphone authentication method based on gait patterns and keystroke dynamics," J. Ambient Intell. Humaniz. Comput., vol. 10, no. 11, pp. 4417–4430, 2019.

[11] Y. Liang, S. Samtani, B. Guo, and Z. Yu, "Behavioral biometrics for continuous authentication in the Internet-of-Things era: An artificial intelligence perspective," IEEE Internet Things J., vol. 7, no. 9, pp. 9128–9143, 2020.

[12] S. Y. Lim, P. T. Fotsing, A. Almasri, O. Musa, M. L. M. Kiah, T. F. Ang, and R. Ismail, "Blockchain technology the identity management and authentication service disruptor: A survey," Int. J. Adv. Sci. Eng. Inf. Technol., vol. 8, no. 4-2, pp. 1735–1745, 2018.

[13] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K.-K. R. Choo, "Blockchain-based identity management systems: A review," J. Netw. Comput. Appl., vol. 166, Art. no. 102731, 2020.

[14] N. Naik and P. Jenkins, "Self-sovereign identity specifications: Govern your identity through your digital wallet using blockchain technology," in Proc. 8th IEEE Int. Conf. Mobile Cloud Comput. Services Eng. (MobileCloud), 2020, pp. 90–95.

[15] V. Nair, "Becoming data: Biometric IDs and the individual in 'Digital India,'" J. R. Anthropol. Inst., vol. 27, no. 1, pp. 26–42, 2021.

[16] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-factor authentication: A survey," Cryptography, vol. 2, no. 1, Art. no. 1, 2018.

[17] T. Rathee and P. Singh, "A systematic literature mapping on secure identity management using blockchain technology," J. King Saud Univ. Comput. Inf. Sci., vol. 34, no. 8, pp. 5782–5796, 2022.

[18] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, Zero Trust Architecture, NIST Special Publication 800-207, National Institute of Standards and Technology, 2020.

[19] J. Sedlmeir, R. Smethurst, A. Rieger, and G. Fridgen, "Digital identities and verifiable credentials," Bus. Inf. Syst. Eng., vol. 63, no. 5, pp. 603–613, 2021.

[20] A. K. Sharma and C. S. Lamba, "Survey on federated identity management systems," in Recent Trends in Networks and Communications, N. Meghanathan, S. Boumerdassi, N. Chaki, and D. Nagamalai, Eds. Berlin, Germany: Springer, 2010, pp. 509–519.

[21] I. Stylios, S. Kokolakis, O. Thanou, and S. Chatzis, "Behavioral biometrics & continuous user authentication on mobile devices: A survey," Inf. Fusion, vol. 66, pp. 76–99, 2021.

[22] F. Wang and P. De Filippi, "Self-sovereign identity in a globalized world: Credentials-based identity systems as a driver for economic inclusion," Front. Blockchain, vol. 2, Art. no. 28, 2020.

[23] M. Wang and W. Deng, "Deep face recognition: A survey," Neurocomputing, vol. 429, pp. 215–244, 2021.

[24] J. Xu, K. Xue, H. Tian, J. Hong, D. S. L. Wei, and P. Hong, "An identity management and authentication scheme based on redactable blockchain for mobile networks," IEEE Trans. Veh. Technol., vol. 69, no. 6, pp. 6688–6698, 2020.

[25] R. N. Zaeem, K. C. Chang, T.-C. Huang, D. Liau, W. Song, A. Tyagi, M. Khalil, M. Lamison, S. Pandey, and K. S. Barber, "Blockchain-based self-sovereign identity: Survey, requirements, use-cases, and comparative study," in Proc. IEEE/WIC/ACM Int. Conf. Web Intell. (WI-IAT), 2021, pp. 128–135.