FutureX Journal, 17-28
Volume 3 (1), November 2025

Regenesys Education
ISSN: 2959-2798

Redefining Digital Identity in the Age of Human-Machine Integration: A Framework for Ethical Authentication and Autonomy

Prof. Maria Venthan Thuraisingham, Durban University of Technology, Durban, South Africa[1]

Keywords

Digital identity
Continuous authentication
Biometrics
Privacy
human-machine integration
AI ethics
Autonomy

Abstract

As human–machine integration accelerates through artificial intelligence (AI), neural interfaces, wearables, and intelligent environments, the foundations of digital identity are being redefined. Traditional centralised and episodic authentication systems no longer suffice for continuous, context-rich, multi-agent ecosystems. This paper introduces a comprehensive conceptual and technical framework for rethinking identity: ethical, end-to-end, ever-present authentication (E³A). We examine the evolution of identity paradigms, continuous and behavioural authentication technologies, privacy-preserving methods such as differential privacy and federated learning, and global legal standards (GDPR, POPIA, EU AI Act). Finally, we present the E³A architecture and sector-specific applications across healthcare, education, finance, and smart cities, offering a foundation for both ethical governance and autonomy-preserving digital identity systems in the post-human era.

[1] Prof. Maria Venthan can be contacted at: atmventhan@yahoo.com

1. Introduction

Human-machine integration (HMI) is redefining the digital ecosystem, merging physical and cognitive experiences across cyber-physical boundaries. The proliferation of wearable sensors, smart assistants, and AI-driven decision agents poses new questions about identity, autonomy, and ethical accountability. Identity is no longer static; it is fluid, adaptive, and co-constructed by humans and machines. Traditional identity mechanisms rely on episodic logins—username and password combinations validated against a central repository. However, these static models are ill-equipped for continuous authentication in ubiquitous computing environments where agents may act semi-autonomously. Hence, the question "Who are you?" evolves into "Who or what is acting, under what authority, and with what ethical safeguards?"

This paper explores how emerging identity paradigms can adapt to ensure security and autonomy in HMI ecosystems. We propose a layered ethical identity framework, E^3A, that aligns with evolving biometric, behavioural, and contextual authentication technologies.

1. Background: The Evolution of Digital Identity

Digital identity historically emerged from administrative constructs—national ID systems, corporate directories, and login credentials. The rise of federated identity management (e.g., OAuth 2.0, SAML, OpenID Connect) marked the first shift toward cross-platform authentication. Yet, this federation remains centralised, leaving privacy vulnerabilities and limited user control.

1.1 Decentralised Identity Paradigm

Decentralised identifiers (DIDs) and verifiable credentials (VCs) proposed by the W3C allow cryptographically verifiable attestations that users control directly. Unlike traditional identity systems, DIDs disassociate identifiers from centralised authorities. Blockchain-based implementations such as Hyperledger Indy and Sovrin are pioneering examples of self-sovereign identity ecosystems.

1.2 The Post-Human Identity Problem

HMI introduces identities that blend biological and computational agency. Cognitive agents can operate autonomously using delegated permissions. Hence, identity verification must address the following dimensions:

- **Multiplicity:** Humans may operate multiple digital twins or AI assistants;
- **Delegation:** Machines act within delegated scopes;

- **Continuity:** Identity assurance must persist across temporal and contextual boundaries; and
- **Ethics:** Machine autonomy must remain subordinate to human consent and ethical oversight.

These dimensions reshape the semantics of digital identity, demanding frameworks that accommodate trust, autonomy, and continuous adaptation.

2. Continuous Authentication and Contextual Intelligence

Continuous authentication shifts the model from discrete validation to persistent confidence scoring. The objective is not merely to verify identity once but to **sustain trust over time**.

2.1 Modalities

- **Behavioural biometrics:** Keystroke dynamics, touchscreen pressure, and gesture-based signals.
- **Physiological biometrics:** Fingerprint, iris, and facial dynamics with liveness detection.
- **Cognitive biometrics:** EEG patterns, reaction times, and emotional responses.
- **Contextual signals:** Device proximity, geolocation, and environmental patterns.

2.2 Liveness and Presentation Attack Detection

ISO/IEC 30107-3 defines metrics (APCER/BPCER) for evaluating resistance to spoofing. State-of-the-art systems integrate thermal imaging and micro-motion cues to mitigate deepfake attacks.

2.3 Adaptive Confidence and Assurance Streams

Identity confidence is modelled as a stream rather than a static outcome. Risk engines continuously analyse deviations in user behaviour. If anomalies exceed thresholds, systems trigger step-up authentication or restricted operation.

2.4 Edge Computing and Federated Learning

Federated learning (FL) trains authentication models across distributed nodes without centralizing biometric data. Techniques like **secure aggregation** and **differential privacy (DP)** further minimise data leakage.

Equation for differential privacy:

Regenesys Education
ISSN: 2959-2798

$$P(M(D) = S) \leq e^{\epsilon} P(M(D') = S) + \delta$$

where (\epsilon) represents the privacy budget.

2.5 Usability and Ethical Constraints

Excessive monitoring risks eroding user trust. Hence, privacy-preserving continuous authentication must balance security with transparency and consent.

3. Legal and Ethical Context

The regulatory landscape dictates ethical boundaries for identity systems.

3.1 GDPR and UK GDPR

Under Article 9 of the GDPR, biometric data qualifies as *special category* data. Processing requires explicit consent, public interest justification, or legal obligation. **Data protection impact assessments (DPIAs)** are mandated for high-risk biometric systems.

3.2 POPIA (South Africa)

The Protection of Personal Information Act (POPIA) mirrors the GDPR's structure, enforcing lawful processing, minimality, and accountability principles.

3.3 EU AI Act (2024)

The EU AI Act introduces a tiered risk framework. Remote biometric identification (RBI) in public spaces faces prohibitions except for national security or serious crime prevention. The act also mandates fundamental rights impact assessments (FRIAs) for high-risk AI systems.

3.4 IEEE Ethically Aligned Design (EAD)

EAD principles advocate human well-being, transparency, accountability, and bias prevention. The emerging IEEE 7000 series (7000–7013) codifies ethics into engineering workflows.

4. The E³A Framework: Ethical, End-to-End, Ever-Present Authentication

4.1 Principles

1. **Autonomy by design:** Users retain control over their identifiers, data, and delegation scopes.
2. **Continuous assurance:** Identity confidence updates dynamically based on context and

behaviour.

3. **Privacy as architecture:** Data minimisation, encryption, and on-device inference are baseline controls.
4. **Delegation accountability:** AI agents act under cryptographically verifiable delegation.
5. **Interoperability by standards:** Built upon SP 800-63-3, FIDO2/WebAuthn, ISO 24760-1, and DIDs.
6. **Ethical governance:** Mandatory oversight through audit trails, fairness metrics, and explainability.

4.2 Architectural Layers

1. **Trust substrate:** Hardware roots (TPMs, secure enclaves).
2. **Authentication layer:** FIDO2 devices, biometric sensors, and PAD.
3. **Identity graph layer:** DID-based credentials and selective disclosure mechanisms.
4. **Assurance orchestrator:** AI-driven risk engine managing assurance streams.
5. **Delegation control:** Scoped credentials for AI/IoT agents.
6. **Audit and ethics layer:** Immutable logging, FRIA, and ethics board oversight.

4.2.1 *Detailed Framework Interpretation*

Each layer within the E³A architecture functions as a modular assurance mechanism:

- **Trust substrate:** Implements hardware-backed roots of trust such as TPM and TEE. These provide tamper resistance and secure key storage, essential for continuous verification;
- **Authentication layer:** Uses multi-modal biometrics and behavioural data. Through Privacy by Architecture, raw biometrics never leave the device, reducing exposure risk;
- **Identity graph layer:** Maintains relationships among human, AI, and IoT identities through verifiable credentials (VCs). This enables contextual identity resolution while maintaining decentralisation;
- **Assurance orchestrator:** Functions as the system's "risk brain," continuously evaluating signals from the environment and user behaviour to adjust access privileges dynamically;
- **Delegation control**: Critical in post-human ecosystems, this ensures machine agents act only

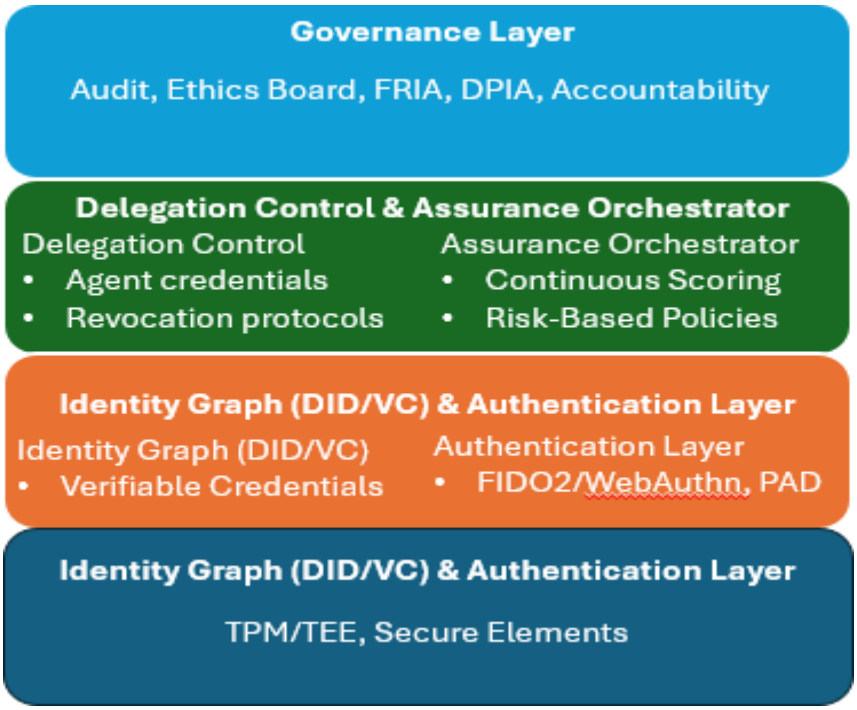
within human-approved scopes. It provides cryptographically bound accountability; and

- Audit and ethics layer: Provides transparency through immutable logs and integrates fairness and responsibility impact assessments (FRIA) for continuous ethical oversight.

This layered design ensures **security, transparency, and human autonomy** remain in equilibrium—the three pillars of the E³A vision.

4.3 Framework Architecture Diagram (Textual Representation)

Figure 1. E³A Framework Architecture



The E³A framework is structured into four governance layers, each ensuring ethical, technical, and operational assurance. The top "Governance Layer" enforces audit, ethics board review, and accountability. The mid-layers handle identity management, delegation, and continuous scoring. The foundational "Trust Substrate" ensures secure execution within trusted hardware.

Regenesys Education
ISSN: 2959-2798

4.4 Authentication Flow Diagram (Textual Representation)

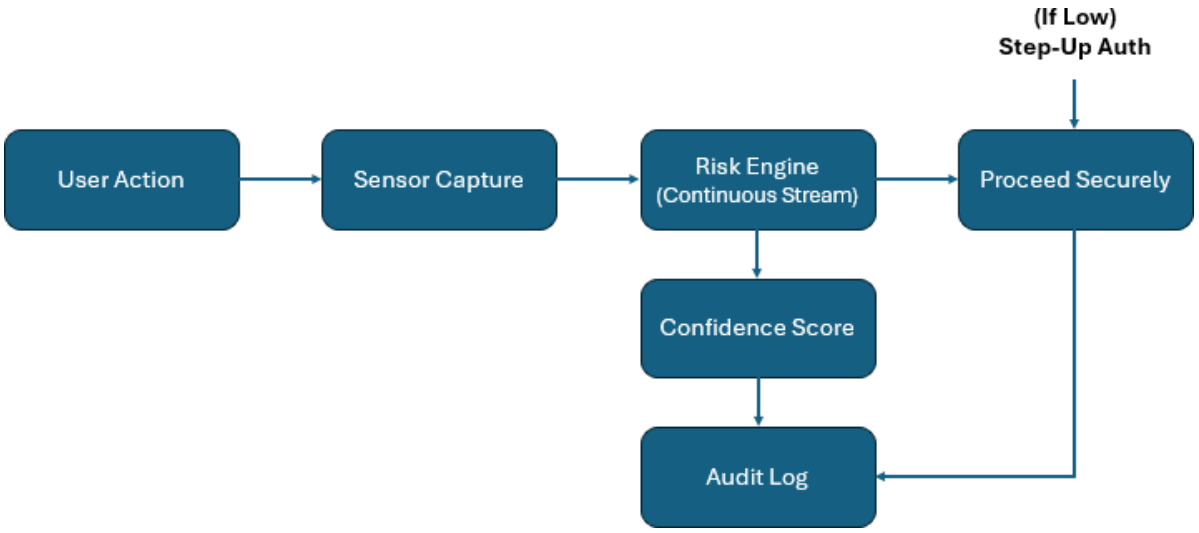


Figure 2: Dynamic cycle of continuous identity

The flow depicts the dynamic cycle of continuous identity assurance. User actions are captured by sensors and processed locally for inference. The risk engine evaluates these signals, generating a confidence score. If the score drops, step-up authentication occurs; otherwise, access proceeds securely and is logged for audit traceability.

4.5 Ethics Integration Workflow

Ethical checkpoints occur during:

- **Design:** DPIA/FRIA initiation;
- **Development:** Bias evaluation in biometric models;
- **Deployment:** Explainable outputs and user opt-out; and
- **Review:** Periodic ethical audits.

5. Applications of E³A Framework

5.1 Healthcare

E³A enables context-aware clinician authentication, continuous session assurance, and privacy-preserving patient monitoring. Credentials can be DID-based, supporting selective disclosure (e.g.,

proving medical licence without exposing personal details).

5.2 Higher Education

Institutions can deploy pseudonymous authentication for coursework while enforcing step-up authentication for assessments. Verifiable credentials replace physical certificates, enhancing portability and verification integrity.

5.3 Banking and Finance

Continuous authentication reduces fraud risk in online banking. Agents (e.g., robo-advisors) operate under restricted delegation credentials. Federated analytics prevent centralisation of biometric data.

5.4 Public Sector and Smart Cities

Citizens authenticate via SSI wallets to access e-services, while anonymised, unlinkable identifiers prevent mass surveillance. Ethical audit layers ensure public accountability.

5.5 Metaverse and Extended Reality (XR)

Users manage multiple virtual identities through DID anchors. PAD ensures avatars correspond to legitimate entities. Behavioural biometrics verify continuity across sessions.

5.6 Real-Life Case Illustrations

- *Healthcare example—Mayo Clinic (USA):*

Mayo Clinic has piloted **continuous authentication for clinicians** using behavioural biometrics combined with wearable sensors. Doctors remain authenticated as long as their gait, heart rate variability, and workstation proximity remain consistent. Once deviations are detected, a step-up authentication request is triggered. This aligns with the **E³A principle of continuous assurance**.

- *Banking example—HSBC (UK):*

HSBC implemented voice biometrics and behavioural pattern analytics for online banking customers, reducing fraud by 50% while maintaining user trust. The system exemplifies delegation accountability, where AI-based fraud detection agents operate within verifiable, limited authority.

- *Smart city example—Singapore Smart Nation Initiative:*

Singapore integrates self-sovereign identity (SSI) wallets for public service access. Citizens authenticate through decentralised credentials while maintaining privacy through selective disclosure. This approach operationalises ethical governance within the E³A framework.

- *Education example—University of Melbourne:*

The university uses blockchain-based digital certificates linked to decentralised IDs. Students' credentials are tamper-proof and verifiable globally, ensuring trust and autonomy, a direct application of E³A's interoperability principle**.**

Table 1: Examples of E³A Implementation

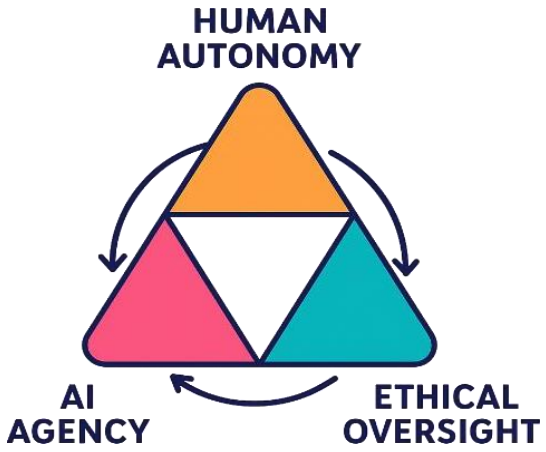
Sector	**E³A Implementation**	**Ethical Consideration**	**Outcome**
Healthcare	Continuous biometric login via wearables	Patient privacy, consent	Reduced impersonation, improved trust
Education	Blockchain-based certificates	Transparency, fairness	Tamper-proof credentialing
Finance	Risk-based behavioural analytics	Delegation control	Reduced fraud, accountability
Smart Cities	SSI wallet integration	Data minimisation	Enhanced citizen autonomy
Metaverse	Behavioural biometrics for avatars	Identity authenticity	Continuity across digital realms

Source: Author's own compilation

7. Discussion: Identity, Autonomy, and Ethical Implications

The interplay between human autonomy and machine agency challenges classical notions of identity. Ethical risks include algorithmic bias, consent fatigue, and identity commodification. Therefore, digital identity governance must evolve toward transparency, proportionality, and human oversight. Autonomous agents necessitate *traceable accountability* while protecting user privacy. Trust in post-human identity systems requires open standards, verifiable credentials, and oversight mechanisms that prioritise dignity and justice. *Figure 3* (following) illustrates the dynamic equilibrium between human autonomy, AI agency, and ethical oversight as three interdependent forces shaping digital identity governance in human–machine ecosystems.

Figure 3. Ethical Balance in Post-Human Identity Systems



Source: Author's own work (2025)

As shown in *Figure 3*, the Ethical Balance Triangle illustrates how human autonomy, AI agency, and ethical oversight continuously interact to maintain responsible digital identity governance in post-human ecosystems. Table 2 (below) summarises the contribution of each component of the ethical triangle.

Table 2: Interaction Roles Within the Ethical Balance Model

Model component	**Role in post-human digital identity**
Human autonomy	Ensures meaningful agency, informed consent, and user control across hybrid human–machine environments.
AI agency	Enables delegated actions with controlled autonomy while enforcing boundaries through technical and ethical safeguards.
Ethical oversight	Provides governance, transparency, auditability, and accountability to prevent misuse, discrimination, or system drift.

7. Conclusion and future work

In a post-human era of blended cognition, digital identity transcends authentication; it becomes a moral and socio-technical contract. The E³A framework advances this redefinition by combining security, ethics, and autonomy into a unified model. By embedding continuous assurance, privacy-by-design, and ethical oversight, we lay the foundation for a trustworthy identity paradigm that empowers rather than constraints. There can be numerous future research ideas in this field. *First*, formal identity grammars to express nested delegation relationships. *Second*, differentially private federated biometrics enabling privacy-preserving adaptation. *Third*, cross-domain SSI interoperability in multi-jurisdictional deployments and bias-resilient liveness detection against adversarial deepfakes. *Fourth*, legal theory of hybrid personhood addressing agency in AI-human collectives.

References

Al-Fedaghi, S. (2021). Conceptualizing the identity lifecycle: A framework for personal data flow. *Journal of Information Privacy and Security, 17*(3), 130–149. https://www.researchgate.net/publication/224638434_Aspects_of_Personal_Information_Theory

Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. *Foundations and Trends in Theoretical Computer Science, S*(3–4), 211–407. https://doi.org/10.1561/0400000042

European Commission. (2024). Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (AI Act*).* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689#:~:text=The%20purpose%20of%20this%20Regulation,explicitly%20authorised%20by%20this%20Regulation.

European Union. (2016). General Data Protection Regulation (GDPR) (Regulation EU 201c/c7S). *Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2016/679/oj*

FIDO Alliance. (2024). *FIDO2: Passwordless authentication standards overview.* Retrieved from https://fidoalliance.org

Floridi, L. (2023). Digital ethics and the post-human condition. *Philosophy & Technology, 3c*(1), 11–32. https://doi.org/10.1007/s13347-022-00550-5

IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems. (2022). *Ethically aligned design (Version II).* https://standards.ieee.org/wp-content/uploads/import/documents/other/ead_v2.pdf

IEEE Standards Association. (2023). *IEEE 7000–2023: Model process for addressing ethical concerns during system design.* https://standards.ieee.org/news/ieee-7000/

International Organization for Standardization. (2023). *ISO/IEC 30107-3: Biometric presentation attack detection—Part 3: Testing and reporting.* https://webstore.iec.ch/en/publication/81714

International Organization for Standardization. (2025). *ISO/IEC 247c0-1: Framework for identity management.* https://www.iso.org/standard/24760-1

Jain, A. K., Ross, A., & C Nandakumar, K. (2021). *Introduction to biometrics* (2nd ed.). Springer. https://link.springer.com/chapter/10.1007/978-981-99-1377-0_26

Kesan, J. P., Hayes, C., & Bashir, M. (2022). Privacy-preserving identity management for the Internet of Things. *Computer Law & Security Review, 47,* 105739. https://doi.org/10.1016/j.clsr.2022.105739

McMahan, H. B., et al. (2017). Communication-efficient learning of deep networks from decentralized data. *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS 2017). https://proceedings.mlr.press/v54/mcmahan17a?ref=https://githubhelp.com*

National Institute of Standards and Technology. (2017). *Digital identity guidelines (NIST Special Publication 800-c3-3).* https://doi.org/10.6028/NIST.SP.800-63-3

Pala, S., & Birhanu, D. (2024). Continuous authentication based on behavioral biometrics: An overview. *Computers & Security, 13S,* 103858. https://doi.org/10.1016/j.cose.2023.103858

Republic of South Africa. (2013). Protection of Personal Information Act (Act No. 4 of 2013). *Government Gazette*. https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf

Rodrigues, J. J. P. C., et al. (2023). Continuous biometric authentication systems: Challenges, advances, and open issues. *IEEE Access, 11,* 14532–14554. https://doi.org/10.1109/ACCESS.2023.3241419

van der Berg, B., & Dignum, V. (2023). Responsible AI and digital identity: A governance perspective. *AI and Ethics, 3*(4), 805–818. https://doi.org/10.1007/s43681-023-00208-9

World Wide Web Consortium. (2023). *Decentralized identifiers (DIDs) v1.0.* W3C Recommendation. Retrieved from https://www.w3.org/TR/did-core/

Zwitter, A., & Gstrein, O. J. (2022). Big data, privacy and COVID-19: Redefining digital identity in crisis. *Ethics and Information Technology, 24*(2), 153–168. https://doi.org/10.1186/s41018-020-00072-6