European Journal of Computer Science and Information Technology, 13(45)99-110, 2025
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Digital Identity in the Modern Era: Navigating the Nexus of Security, Privacy, and Social Inclusion

Karanveer Singh Gondara
Punjabi University, Patiala, India

doi: https://doi.org/10.37745/ejcsit.2013/vol13n4599110 Published June 26, 2025

Citation: Gondara K.S. (2025) Digital Identity in the Modern Era: Navigating the Nexus of Security, Privacy, and Social Inclusion, *European Journal of Computer Science and Information Technology*, 13(45)99-110

Abstract: *Digital identity systems have become central to the functioning of modern digital economies and governance structures. With the proliferation of national ID programs and global digital identity initiatives, questions of data security, user privacy, and social inclusion have risen to the forefront. This paper explores the evolving landscape of digital identity, examining the balance between technological advancement and ethical responsibility. It presents a comparative view of global identity programs, including India's Aadhaar and the EU's eIDAS framework, alongside emergent models like decentralized and self-sovereign identity (SSI). Emphasis is placed on the role of identity transformation in enterprise cybersecurity and the integration of governance automation to ensure scalable, compliant, and inclusive identity architectures. The paper concludes with strategic considerations for designing equitable digital identity systems that respect individual rights while meeting operational demands.*

Keywords: digital identity, data privacy, authentication security, digital inclusion, identity governance

INTRODUCTION

The Evolving Landscape of Digital Identity

In the rapidly evolving digital age, the concept of identity has transcended physical documents and face-to-face verification. Today, digital identity is at the heart of not just access management and enterprise security but also plays a pivotal role in civic participation, financial inclusion, and service delivery [1]. As societies become increasingly digitized, the tension between security, privacy, and inclusion in digital identity ecosystems grows more pronounced. While digital identity offers the promise of frictionless services, simplified authentication, and enhanced security, it also raises concerns around surveillance, data misuse,

exclusion, and loss of autonomy [5]. The design and governance of these systems determine whether they empower users or entrench systemic inequities.

Defining Digital Identity in the Contemporary Context

Digital identity in the contemporary context represents far more than simple authentication credentials. It encompasses the comprehensive collection of attributes, credentials, and interactions that define an individual in digital environments [1]. These digital representations have evolved from basic usernames and passwords into complex ecosystems incorporating biometric data, behavioral patterns, and digitized official documents. This evolution has transformed how individuals establish trust and verify their personhood across digital platforms.

Historical Development and Current Prevalence

The historical development of digital identity systems traces back to early computer network access controls, progressing through increasingly sophisticated authentication mechanisms. Early systems relied primarily on knowledge factors—what a user knows—while contemporary frameworks incorporate possession factors (devices) and inherence factors (biometrics) [4]. This progression reflects broader technological advances and shifting security paradigms. The current prevalence of digital identity solutions spans from enterprise access management to consumer applications and government-issued credentials, creating an intricate web of identity systems that individuals must navigate daily.

The Rise of Global Identity Programs

Governments and enterprises globally are investing in digital identity platforms. For example, India's Aadhaar program, a biometric-based national ID system, has enrolled over a billion individuals [11]. While Aadhaar has facilitated access to welfare programs and banking, it has also drawn scrutiny over privacy breaches and lack of meaningful user consent. The European Union's eIDAS regulation aims to create a unified and interoperable digital identity framework across member states, emphasizing security, legal validity, and user control [10]. Meanwhile, countries like Estonia and Singapore are pioneering identity-as-a-service models with built-in transparency and portability.

Growing Reliance on Digital Identity Systems for Essential Services

The growing reliance on digital identity for essential services marks a significant shift in how societies function. Financial services, healthcare, education, and government benefits increasingly require robust digital verification before granting access [5]. This dependency creates new paradigms of inclusion and exclusion based on digital identity capabilities. National identity systems now extend beyond traditional identification purposes into functional capabilities like digital signing [2], highlighting this deepening integration into civic infrastructure.

The Need for Balanced Approaches to Digital Identity

This article argues that as digital identity becomes the gateway to fundamental rights and services, a balanced approach must guide its implementation—one that harmonizes security imperatives with privacy protections while ensuring universal accessibility [15]. The tension between these competing interests requires thoughtful design choices, governance frameworks, and technological solutions that prioritize human dignity and agency while meeting legitimate security needs. Addressing these challenges demands interdisciplinary collaboration across technical, legal, ethical, and social domains to create identity systems that serve rather than subvert human flourishing.

Security Imperatives and Verification Methodologies

Current Verification Technologies and Their Efficacy

Digital identity systems employ a diverse array of verification technologies, each with distinct security properties and user experience implications. These technologies span from traditional knowledge-based approaches to advanced cryptographic methods and artificial intelligence-driven systems. The efficacy of these verification mechanisms must be evaluated against multiple criteria: resistance to forgery, scalability, performance, and adaptability to emerging threats. Security guidelines for these technologies require formal specification to ensure consistent implementation across systems and organizations [3]. The verification landscape continues to evolve as both legitimate users and malicious actors gain technological sophistication, necessitating continuous reassessment of efficacy metrics.

Table 1: Comparison of Digital Identity Verification Methods [3, 4]

Verification Method	Security Level	User Experience	Accessibility Challenges
Knowledge-based	Moderate	Familiar	Cognitive limitations
Biometric	High	Seamless	Physical disabilities
Multi-factor	Very high	Added steps	Digital literacy, device dependency
Risk-based	Adaptive	Context-dependent	Algorithmic bias potential
Token-based	High	Requires possession	Device access, cost barriers

Biometric Authentication: Strengths and Vulnerabilities

Biometric authentication leverages physiological or behavioral characteristics unique to individuals, offering convenience while potentially enhancing security [13]. Fingerprints, facial recognition, iris scans, and voice patterns have become commonplace in identity verification contexts. These methods provide advantages in usability by removing the need to remember complex passwords. However, they introduce

distinct vulnerabilities, including spoofing attacks, template theft risks, and challenges with revocation when compromised. Additionally, biometric systems face accuracy challenges with false acceptance and rejection rates that must be balanced according to use context. Permanent biological characteristics also raise specific privacy concerns absent in traditional authentication methods, as they cannot be changed if compromised.

Multi-factor Authentication and Risk-based Approaches

Multi-factor authentication (MFA) has emerged as a cornerstone strategy in identity security, combining elements from different authentication categories: knowledge factors (passwords), possession factors (devices), and inherence factors (biometrics) [4]. This layered approach substantially increases security by requiring attackers to compromise multiple authentication channels simultaneously. Risk-based authentication extends this concept by dynamically adjusting security requirements based on contextual factors such as location, device characteristics, behavioral patterns, and transaction risk levels [13]. These adaptive approaches enable security teams to apply appropriate protections without unnecessarily burdening users during low-risk interactions, thereby balancing security with usability.

Case Studies of Major Security Breaches and Lessons Learned

Significant security breaches involving identity systems provide valuable insights into vulnerability patterns and mitigation strategies. Notable incidents have demonstrated how single-factor authentication failures, social engineering attacks, and implementation flaws can compromise even sophisticated identity infrastructures [1]. These breaches have revealed common patterns: over-reliance on perimeter defenses, inadequate monitoring of authentication anomalies, and insufficient protection of credential databases. The lessons learned emphasize the importance of defense-in-depth strategies, regular security assessments, encryption of identity data at rest and in transit, and comprehensive security awareness training. Organizations increasingly recognize that technical controls must be complemented by organizational processes and security culture to create truly resilient identity ecosystems.

Privacy Concerns and Data Governance

Personal Data Collection, Storage, and Sharing Practices

Digital identity systems necessitate extensive collection of personal information, raising significant privacy implications. These systems typically gather identifying information ranging from basic biographical data to sensitive biometric markers and behavioral patterns. Storage architectures vary from centralized repositories to distributed ledgers, each presenting distinct privacy risk profiles [5]. Data minimization principles suggest collecting only essential information for identity verification, yet commercial and governmental systems often extend beyond these boundaries. Sharing practices between identity providers and relying parties create complex data flows that may obscure accountability and increase vulnerability surfaces. The ethical dimensions of these practices require careful consideration beyond mere legal compliance, particularly as digital identity becomes mandatory for accessing essential services [5].

Regulatory Frameworks

The global landscape of identity-related privacy regulation has evolved rapidly in response to growing concerns about data protection. Major regulatory frameworks have established new paradigms for consent, transparency, and individual rights regarding personal data [6]. These regulations differ significantly in scope, enforcement mechanisms, and fundamental approaches to privacy. Some jurisdictions emphasize individual control and explicit consent, while others focus on organizational accountability and data stewardship. The global patchwork of regulations creates compliance challenges for cross-border identity systems while establishing baseline protections for individuals [6]. Regulatory developments continue to evolve as technological capabilities advance and societal expectations around privacy shift.

Table 2: Major Regulatory Frameworks Governing Digital Identity [5, 6]

Regulation	Jurisdictional Scope	Key Identity Provisions	Consent Model
GDPR	European Union	Data minimization	Explicit, opt-in
CCPA/CPRA	California, USA	Right to know/delete	Opt-out
Digital Identity Acts	Various countries	Digital signatures	Varies
eIDAS	European Union	Cross-border recognition	Tiered assurance
Privacy Act amendments	Multiple regions	Biometric protections	Enhanced consent

Data Ownership Models and User Control Mechanisms

Competing models of data ownership underpin digital identity systems, influencing their privacy and control characteristics [12]. Traditional models often place primary control with identity providers or relying parties, while emerging approaches emphasize user-centric governance. Self-sovereign identity frameworks attempt to rebalance control toward individuals through technical architectures that enable selective disclosure and verifiable credentials without continuous provider involvement [9, 17]. User control mechanisms include consent management dashboards, data portability tools, personal data stores, and revocation capabilities. These mechanisms vary in their effectiveness, usability, and genuine ability to shift power dynamics in favor of individuals. The implementation of these control systems often struggles to balance comprehensive oversight with cognitive accessibility.

Surveillance Capitalism and State Surveillance Implications

Digital identity systems exist within broader contexts of commercial and governmental surveillance capabilities. Commercial entities may leverage identity data for behavioral profiling, predictive analytics, and targeted advertising—hallmarks of surveillance capitalism [5]. Simultaneously, state actors may utilize these systems for social control, population management, and intelligence gathering. The dual pressures from commercial and state surveillance create complex tensions within identity architectures. Privacy-enhancing technologies attempt to mitigate these surveillance risks through cryptographic techniques, decentralization, and purpose limitations [12]. However, the fundamental power asymmetries between

individuals and institutions—both governmental and commercial—present ongoing challenges for privacy-preserving identity solutions that resist surveillant applications.

Digital Equity and Inclusion Challenges

Digital Identity Gaps Across Socioeconomic Divides

The implementation of digital identity systems reveals persistent gaps that mirror and sometimes amplify existing socioeconomic divides. These systems frequently presuppose access to digital infrastructure, technological literacy, and documentation that remain unevenly distributed across populations. The technological prerequisites for digital identity—smartphones, reliable internet connectivity, and digital literacy—create stratified access patterns that correlate with income, education, and geographic location. As Warschauer [7] emphasizes, technology access alone fails to address deeper structural inequalities that determine meaningful participation in digital environments. When essential services increasingly require digital identity verification, these gaps transform from inconveniences into substantial barriers to social and economic participation, potentially creating new forms of exclusion.

Barriers to Access for Marginalized Communities

Marginalized communities face multidimensional barriers to digital identity systems beyond simple technology access. These barriers include limited digital literacy, language obstacles, cultural mistrust of governmental or corporate systems, historical exclusion from formal identification systems, and accessibility challenges for persons with disabilities [8]. Documentation requirements often disadvantage homeless populations, refugees, and internally displaced persons who lack stable addresses or formal credentials. Furthermore, identity systems designed without consideration for diverse literacy levels, disability accommodations, or cultural contexts inadvertently exclude segments of society. These barriers create compounding disadvantages when digital identity becomes mandatory for accessing healthcare, financial services, education, and social benefits.

Alternative Verification Approaches for Underserved Populations

Addressing inclusion challenges requires developing alternative verification approaches tailored to the circumstances of underserved populations [15]. These include tiered identity assurance models that accommodate varying levels of documentation, proxy systems that allow trusted intermediaries to vouch for individuals lacking credentials, and offline verification methods for regions with limited connectivity. Community-based enrollment campaigns, mobile registration units, and simplified enrollment processes can increase accessibility for remote or marginalized communities. Additionally, multimodal interfaces that accommodate varying literacy levels and abilities, alongside non-digital fallback mechanisms, maintain access for those who cannot navigate purely digital solutions. These approaches recognize that inclusion requires flexibility rather than rigid standardization across diverse contexts.

European Journal of Computer Science and Information Technology, 13(45)99-110, 2025
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Global Perspectives: Developing vs. Developed World Implementations

Digital identity implementations reveal significantly different challenges and opportunities across global contexts [8]. Developed economies typically build digital identity upon established identification infrastructure, focusing on digitizing existing credentials, enhancing privacy protections, and integrating across service domains. Conversely, developing regions often implement digital identity systems to address fundamental identification gaps, sometimes leapfrogging paper-based systems entirely [11]. These divergent starting points create different risk profiles and success metrics. Implementation models from high-resource environments frequently require adaptation for contexts with limited infrastructure, different privacy expectations, and unique cultural norms around identity. International cooperation frameworks attempt to balance innovation with contextual appropriateness, recognizing that imported models can fail without adaptation to local conditions.

Emerging Standards and Best Practices

Self-Sovereign Identity Models and Decentralized Approaches

Self-sovereign identity (SSI) represents a paradigm shift in digital identity management, placing individuals at the center of control over their identity information [17]. This approach fundamentally reconfigures the relationship between identity holders, issuers, and verifiers through cryptographic mechanisms that enable selective disclosure and verification without continuous issuer involvement. SSI models typically utilize distributed ledger technologies to establish trust anchors while keeping personal data off-chain [9]. These systems allow individuals to maintain collections of verifiable credentials from various issuers, presenting only necessary information to service providers without revealing irrelevant attributes [12]. The architectural principles behind SSI emphasize persistent, portable identities that exist independent of any specific provider or platform. As Preukschat and Reed [9] explore, these decentralized approaches aim to address fundamental power imbalances in traditional identity ecosystems by embedding privacy and user control into the technical architecture itself.

European Journal of Computer Science and Information Technology, 13(45)99-110, 2025
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

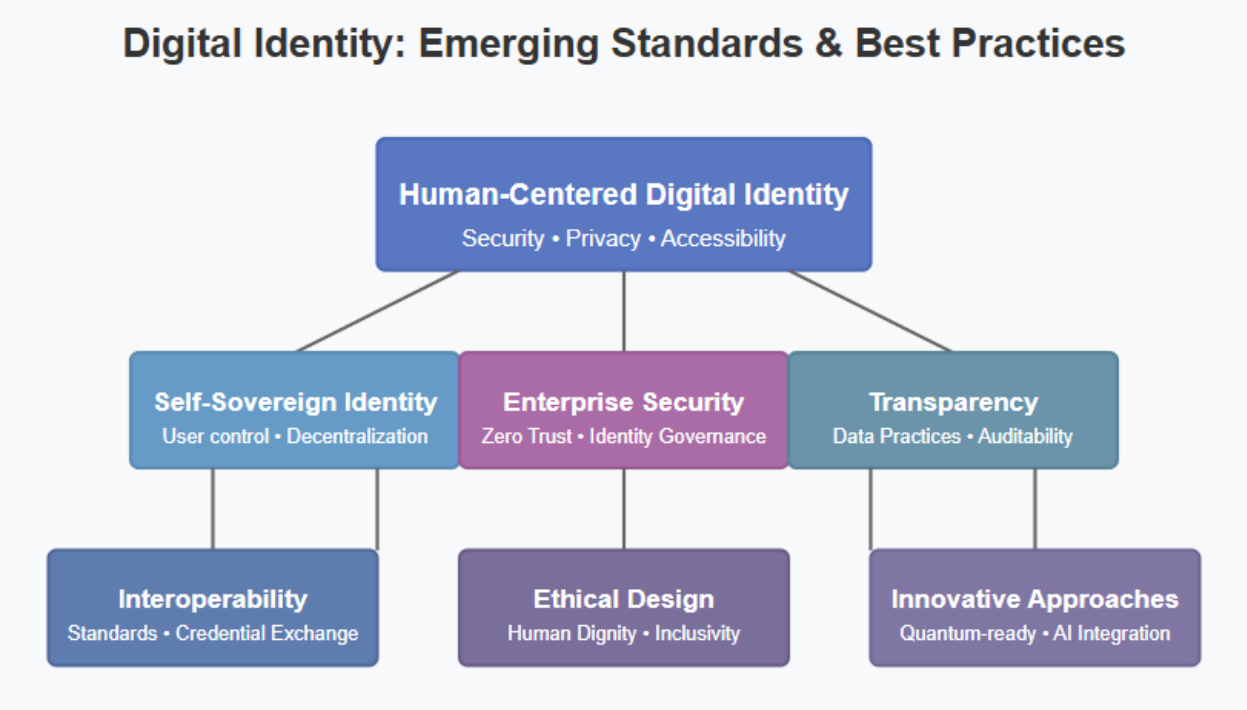

Fig: Digital Identity Framework: A hierarchical view of human-centered approaches encompassing self-sovereignty, enterprise security, and ethical design principles with key implementation standards.

Table 3: Self-Sovereign Identity Implementation Approaches [9]

SSI Component	Technical Implementation	User Control Feature	Standard
Decentralized Identifiers	Distributed ledgers	Provider independence	W3C DID
Verifiable Credentials	Signed claims	Selective disclosure	W3C VC
Identity Wallets	Mobile/desktop apps	Credential management	DIDComm
Trust Registries	Permissioned ledgers	Issuer verification	ToIP
Zero-knowledge Proofs	Cryptographic protocols	Minimal disclosure	ZKP

Enterprise Cybersecurity and Identity Transformation

In the enterprise context, identity is the new perimeter. The transition to cloud, hybrid work models, and Zero Trust security paradigms has accelerated the need for robust Identity Governance and Administration (IGA) [14]. Organizations are moving from traditional role-based models to dynamic, context-aware identity systems.

Identity transformation entails modernizing legacy identity architectures and embracing automation, analytics, and AI to enforce least-privilege access [16]. This includes integration of tools like Microsoft Entra ID, SailPoint, and Saviynt, as well as federated identity frameworks using SAML, OAuth2.0, and OpenID Connect. Leading ERP transformations, such as SAP ERP upgrades with integrated SAP GRC (Governance, Risk, and Compliance), demonstrate how identity and access policies can be operationalized across complex, interconnected environments [14]. Automating access reviews, segregation of duties (SoD), and policy enforcement improves security posture while meeting compliance mandates.

Interoperability and Portability Considerations

Interoperability between identity systems has emerged as a critical requirement for functional digital ecosystems [10]. Technical standards including verifiable credentials, decentralized identifiers (DIDs), and credential exchange protocols create foundations for cross-system compatibility [12]. These standards enable credentials issued in one context to be verified seamlessly in another, reducing fragmentation that forces individuals to maintain multiple disparate digital identities. Portability—the ability to transfer identity assets between providers—complements interoperability by preventing vendor lock-in and enhancing user autonomy. Implementation challenges include navigating competing standards, ensuring cryptographic compatibility, and establishing governance frameworks that incentivize adoption while maintaining security. International standards bodies continue developing specifications that balance innovation with interoperability, recognizing that isolated identity silos undermine both user experience and system resilience.

Transparency and Auditability Requirements

Transparency in digital identity systems encompasses clear communication about data collection, processing, sharing practices, and algorithmic decision-making [15]. This transparency extends to both technical operations and governance structures, enabling informed consent and accountability. Auditability requirements complement transparency by creating mechanisms to verify compliance with stated policies and detect unauthorized modifications or access. Technical approaches include immutable logs of consent decisions, cryptographic proofs of data integrity, and independent verification of system operations. These mechanisms serve both regulatory compliance needs and broader legitimacy concerns by enabling independent validation of system behavior. The tension between comprehensive transparency and necessary confidentiality requires careful calibration, particularly regarding security mechanisms where some opacity may be operationally necessary.

Ethical Design Frameworks and Governance Models

Ethical design frameworks for digital identity increasingly incorporate principles of human dignity, autonomy, fairness, and inclusion from initial conceptualization through implementation and operation [15]. These frameworks emphasize participatory design approaches that include diverse stakeholders, particularly those most vulnerable to identity-related harms. Governance models range from traditional centralized authorities to multi-stakeholder structures and decentralized autonomous organizations.

Effective governance balances technical expertise with democratic legitimacy and adaptation mechanisms that respond to evolving social norms and technological capabilities.

Technology must not outpace ethics [5]. Vulnerable populations—including migrants, the unbanked, and those without traditional documentation—often face exclusion in rigid identity systems [8]. Ethical identity design mandates user agency, minimal data collection, and redress mechanisms. Public-private collaboration, inclusive policy-making, and ongoing oversight are vital [15]. Identity systems should accommodate edge cases and respect cultural and contextual diversity.Independent oversight bodies, certification mechanisms, and regular ethical impact assessments help maintain alignment with human rights standards and societal values. These governance approaches recognize that digital identity systems embody power structures that require deliberate ethical consideration rather than treating them as neutral technical implementations.

CONCLUSION

The evolution of digital identity systems represents a pivotal societal transformation with profound implications for individual rights, collective governance, and institutional power structures. These systems embody inherent tensions between security imperatives, privacy considerations, and accessibility requirements that resist simplistic resolutions. Moving forward, the development of truly human-centered digital identity frameworks necessitates multidisciplinary collaboration that integrates technical innovation with ethical principles, regulatory frameworks, and inclusive design practices. Self-sovereign and decentralized models offer promising directions for rebalancing power relationships, yet require careful governance to prevent replicating existing inequities in new forms. The global nature of these challenges demands international cooperation alongside contextual adaptation to diverse socioeconomic realities.

As we look toward the horizon of digital identity evolution, several critical developments warrant attention from researchers, policymakers, and practitioners. The integration of artificial intelligence in identity systems introduces new possibilities for adaptive authentication and fraud detection, but also raises profound questions about algorithmic bias, explainability, and human oversight. Similarly, the looming quantum computing era necessitates fundamental reconsideration of cryptographic foundations underpinning current identity infrastructures. Developing quantum-resistant verification methods while maintaining usability and accessibility represents a significant technical and design challenge that requires proactive attention.

The metaverse and extended reality environments further complicate identity paradigms, as digital representation becomes increasingly multifaceted and persistent across virtual contexts. These emerging spaces demand novel approaches to verification, reputation, and governance that balance innovation with protection against new forms of identity-based harms. Additionally, climate considerations must inform the development of identity infrastructures, as the environmental impact of distributed systems and biometric verification mechanisms becomes increasingly relevant in resource-constrained contexts.

The path forward requires bold experimentation balanced with rigorous evaluation. Digital identity sits at the confluence of technological innovation, regulatory complexity, and human rights. To unlock its full potential, stakeholders must design systems that are secure, privacy-preserving, interoperable, and inclusive. The path forward requires a thoughtful integration of governance automation, identity transformation, and ethical foresight.

We call upon technologists to embrace human-centered design principles from inception; for policymakers to develop adaptive, principle-based regulatory frameworks rather than rigid technical mandates; and for civil society to actively participate in shaping identity systems that enhance human capabilities rather than constrain them. Educational institutions must prepare the next generation of practitioners with interdisciplinary perspectives that span technical implementation and ethical governance.

Ultimately, digital identity systems should serve as enablers of human agency and dignity rather than mechanisms of control—a vision requiring continuous engagement from technologists, policymakers, civil society, and the individuals whose fundamental rights are at stake. By centering human needs and values in both the technical architecture and governance frameworks of identity systems, societies can harness their benefits while mitigating their potential to exacerbate existing power imbalances or create new forms of exclusion. Stakeholders must now collaborate to transform this vision into action, advancing identity ecosystems that prioritize trust, equity, and accountability by design.

REFERENCES

[1] Christine Evans-Pughe, "A Crisis of Identity [Engineering Digital Identity]," Engineering & Technology, vol. 3, no. 10, IEEE Xplore, 07 June 2008. https://ieeexplore.ieee.org/document/4621845
[2] Emir Husni, "Digital Signing Using National Identity as a Mobile ID," 2016 International Seminar on Intelligent Technology and Its Applications (ISITIA), IEEE Xplore, 23 January 2017. https://ieeexplore.ieee.org/document/7828668
[3] Zeineb Zhioua, Yves Roudier, et al., "Formal Specification and Verification of Security Guidelines," 2017 IEEE 22nd Pacific Rim International Symposium on Dependable Computing (PRDC), IEEE Xplore, 08 May 2017. https://ieeexplore.ieee.org/document/7920631
[4] Rashad Mahmood Saqib, Adnan Shahid Khan, et al., "Analysis and Intellectual Structure of Multi-Factor Authentication in Information Security," Intelligent Automation & Soft Computing, TechScience, 14 July 2021. https://www.techscience.com/iasc/v32n3/45903/html
[5] IEEE Digital Privacy "Ethical Issues Related to Data Privacy and Security: Why We Must Balance Ethical and Legal Requirements in the Connected World," IEEE Digital Privacy, IEEE. https://digitalprivacy.ieee.org/publications/topics/ethical-issues-related-to-data-privacy-and-security-why-we-must-balance-ethical-and-legal-requirements-in-the-connected-world
[6] IEEE Digital Privacy "Emerging Data Privacy Laws and Regulations Around the World," IEEE Digital Privacy, IEEE. https://digitalprivacy.ieee.org/publications/topics/emerging-data-privacy-laws-and-regulations-around-the-world
[7] Mark Warschauer, "Technology and Social Inclusion: Rethinking the Digital Divide," MIT Press eBooks, IEEE Xplore, 2004. https://ieeexplore.ieee.org/book/6267354

[8] Connecting the Unconnected, IEEE "Impact of the Digital Divide: Economic, Social, and Educational Consequences," Connecting the Unconnected, IEEE, 27 February 2023. https://ctu.ieee.org/blog/2023/02/27/impact-of-the-digital-divide-economic-social-and-educational-consequences/
[9] Alex Preukschat, Drummond Reed, "Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials," IEEE Xplore, 2021. https://ieeexplore.ieee.org/book/10280453
[10] European Commission. (2021). eIDAS Regulation: Regulation (EU) No 910/2014 on electronic identification and trust services. https://digital-strategy.ec.europa.eu
[11] UIDAI. (2023). Aadhaar Dashboard. Unique Identification Authority of India. https://uidai.gov.in
[12] W3C. (2022). Verifiable Credentials Data Model 1.1. https://www.w3.org/TR/vc-data-model/
[13] NIST. (2020). Digital Identity Guidelines (Special Publication 800-63-3). National Institute of Standards and Technology.
[14] Gartner. (2023). Identity Governance and Administration (IGA) Market Guide. Gartner Research.
[15] World Economic Forum. (2021). Principles for Digital Identity. https://www.weforum.org
[16] Microsoft. (2023). Entra Identity Platform Documentation. https://learn.microsoft.com
[17] Sovrin Foundation. (2022). Self-Sovereign Identity (SSI) Overview. https://sovrin.org