JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Formalizing the Academic Digital Identity: A Conceptual Framework for Education in the Digital Age

[1]Swapnil Gaidhani, [2]Dr. Gopal Krishna Sharma
[1]Research Scholar, [2]Assistant Professor
[1]Department of Computer Science,
[1]Dev Sanskriti Vishwavidyalaya, Haridwar, India

Abstract: *The escalating digitization of scholarly practice necessitates a re-evaluation of how academic contributions are formally recognized and accumulated. This conceptual paper conceptualizes and defines "Academic Digital Identity" (ADI), a specialized, user-centric, and verifiable digital framework designed to comprehensively document a scholar's lifelong accolades and professional journey. Drawing insights from India's experience with foundational digital identities and global discussions on fragmented academic digital footprints, this paper articulates the essential elements of ADI. It argues for its distinct purpose by critically analyzing the limitations of current top-down, federated models like India's APAAR ID. By advocating for a Self-Sovereign (SSI) model rooted in verifiable credentials and interoperable standards, this framework aims to address current fragmentation, enhance scholarly visibility, and streamline future academic evaluation, thereby fostering a more equitable and efficient global academic ecosystem.*

Index Terms **- Academic Digital Identity, Self-Sovereign Identity (SSI), Digital Identity, Verifiable Credentials, Researcher Identity, Digital Competence, eIDAS, APAAR ID.**

I. INTRODUCTION

The modern scholarly environment is experiencing a significant metamorphosis, propelled by the ubiquitous incorporation of digital technologies and platforms [1]. Academics are progressively utilizing a diverse array of digital instruments for pedagogical purposes, scholarly inquiry, and interaction, resulting in a context wherein scholarly identity is progressively shaped within the online sphere [2]. This rapid digitization has fostered a complex interaction of opportunities and challenges in the recognition and accumulation of academic contributions. While digital platforms provide unparalleled visibility and collaboration opportunities, the current state of academic digital identity governance remains notably fragmented, insecure, and institution-centric [3].

This fragmentation manifests as a lack of cohesive, universally recognized mechanisms to capture the full spectrum of a scholar's lifelong achievements. Academics are forced to maintain multiple, often incompatible, profiles across various platforms (e.g., institutional repositories, ResearchGate, ORCID, Google Scholar, Twitter) [4], imposing a significant "workload" on academics for profile maintenance [5] and creates a disconnect between these two sorts of measures: ways of knowing and ways of measuring value in academic evaluation [2]. The consequences are significant, leading to incompatible digital identity systems that prevent seamless enrollment, personalized learning pathways, and reliable credential verification" globally [6] and potentially undermining trust in digital identity systems.

This paper addresses this critical gap by conceptualizing and defining the "Academic Digital Identity" (ADI) as a specialized and comprehensive digital identity framework. The primary objective is to formalize a model that can effectively accumulate and verify the countless accolades a scholar earns throughout their academic journey. This paper will first survey the evolving landscape of academic identity to establish a clear knowledge gap. It will then introduce a theoretical justification for a new approach—the principle of contextual specialization. Finally, it will propose a formal ADI framework built on the principles of Self-Sovereign Identity (SSI), outlining its conceptual elements and discussing its transformative implications for a more integrated, secure, and user-controlled environment for academic recognition [7].

II. EVOLVING LANDSCAPE OF ACADEMIC IDENTITY

To contextualize the need for a new framework, it is pertinent to review the evolution of digital identity within academia, from its early conceptualizations to the complex infrastructural and human challenges of today.

2.1 Historical Precedent: ADI as the e-portfolio

The term "academic digital identity" was first formally introduced by Hiradhar et al, 2009 in the context of student e-Portfolios as a transition from a social digital identity to an academic digital identity [8]. This foundational work was crucial in distinguishing the professional and educational aspects of a student's online presence from their social persona However, this early conceptualization was primarily tool-specific, tying the identity to the e-Portfolio system and lacking the comprehensive, interoperable scope required by today's global academic ecosystem.

2.2 Modern Reality: The Fragmented Researcher Identity

As per Andrea et al, 2022, in current practice, a researcher's digital identity is distributed across a patchwork of organizational and commercial platforms, including ORCID, Scopus, Google Scholar, and ResearchGate [9]. While Marques et al, 2024 specifies these services are central to establishing scholarly credit, academics must manually create and update these profiles, a task that has become a form of essential but burdensome academic workload [5]. This fragmentation is exacerbated by the emergence of the "quantified self in academia," which exposes researchers to "an overwhelming array of evaluations and indices." [10], often without their direct control. This management burden is exacerbated by the fact that most academics possess only intermediate digital skills, with pronounced deficiencies in managing digital security and privacy, highlighting the risks for the least digitally savvy in a fragmented environment as shown in **Error! Reference source not found.** [11].

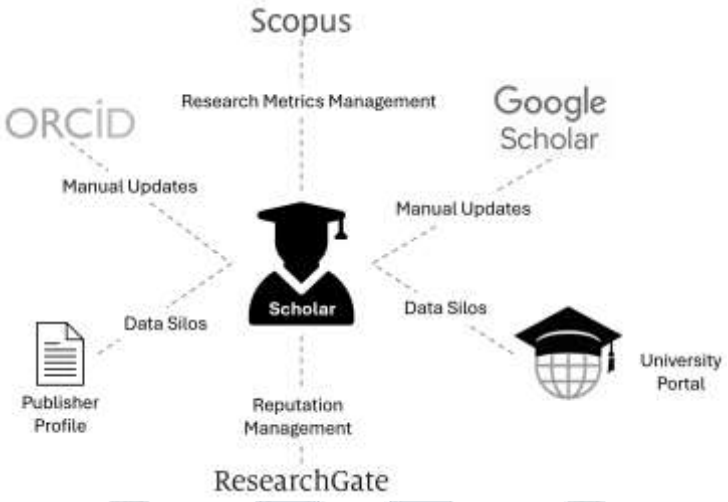

Figure 1 The Fragmented Academic Digital Identity: A Disconnected Ecosystem

2.3 Infrastructural Challenges: Top-Down Federated Models

Recognizing the need for interoperability, governments have launched large-scale identity initiatives. Europe's eIDAS infrastructure created a transnational framework for basic cross-border authentication but was designed with a minimal set of attributes, offering limited granularity for the complex needs of academic credentialing [12].

More recently, India's Automated Permanent Academic Account Registry (APAAR) ID, integrated with the DigiLocker digital wallet, represents an ambitious national-scale solution to domestic fragmentation for over310 million learners [13]. This system enables credential storage and verification within a centralized, government-operated architecture [14]. Critically, however, both eIDAS and APAAR adhere to federated or centralized models. While administratively efficient, they are not natively user-centric, lack flexible portability, and struggle with the global interoperability required for diversified academic and career trajectories.

2.4 Research Gap

The literature reveals a landscape marked by fragmentation, burden, and risk. Early concepts of ADI were tool-specific, while modern practice has led to a fragmented and labor-intensive ecosystem. Meanwhile, top-down infrastructures are not sufficiently user-centric, portable, or globally interoperable. While the literature documents the what (fragmentation) and the why (risks and pressures), it lacks a comprehensive how—a formal, user-centric framework that is architecturally distinct from the federated models that have proven insufficient. This paper proposes such a framework.

III. THE CASE FOR SPECIALIZED, SELF-SOVEREIGN ADI

The justification for a new ADI framework is rooted in two core arguments: the practical precedent of contextual specialization in identity systems and the architectural superiority of a self-sovereign model in addressing the documented failures of centralized systems.

3.1 The Case for Specialized, Self-Sovereign ADI

High-stakes, specialized domains require purpose-built identity frameworks that a general-purpose identity cannot adequately serve. India's digital identity landscape offers a compelling precedent. As shown in **Error! Reference source not found.**, the Aadhaar ID serves as a general-purpose foundational identity for all residents, designed to prove existence and enable access to a wide array of government services [15], [16], [17]. In contrast, the APAAR ID serves as a specialized academic identifier within the same national framework, designed to manage educational records and credit portability [18]. The successful co-existence of these systems demonstrates the practical utility of specialized digital identities. Academia, with its unique set of 'accolades' and distinct validation

mechanisms, is precisely such a specialized domain that warrants its own dedicated identity framework beyond general national identifiers.

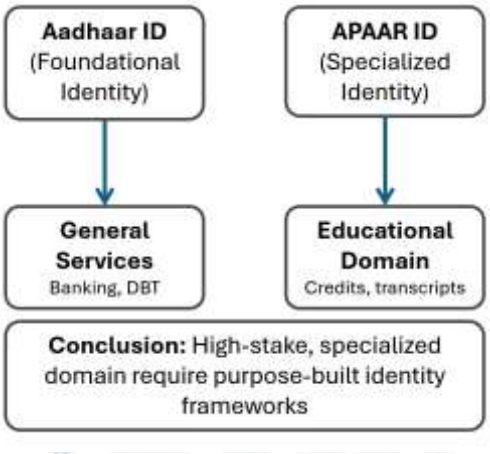

Figure 2 The principle of Contextual Specialization in Digital Identity

3.2 The Limitations of Centralized Models: A Critique of APAAR

While APAAR represents a monumental step in solving domestic fragmentation, its centralized architecture presents fundamental limitations for a truly global and learner-centric academic identity:

- **Institution-Centric Control**: Despite "student-centric" rhetoric, the architecture remains centralized. The student does not have sovereign control over their data; they are granted access to an account within a government-managed system [19].
- **Lack of Global Interoperability:** The system is built on India-specific infrastructure (Aadhaar, NAD). A foreign university or employer cannot cryptographically verify an APAAR credit statement without a pre-established, bespoke integration, limiting students pursuing global opportunities [19].
- **Limited Privacy:** The system relies on platform security and policy, and data aggregation is possible at the central level. It lacks privacy-by-design features like selective disclosure [20]. For instance, the risks of centralized aggregation are not theoretical—high-profile breaches such as the 2020 attack on the University of California, San Francisco's systems underscore the vulnerability of educational data when stored in large, centralized repositories [21].

These limitations are not unique to APAAR but are inherent in all centralized and federated identity models. They can only be solved by a different architectural paradigm: Self-Sovereign Identity (SSI).

IV. Proposing the Academic Digital Identity (ADI) Framework

This paper proposes a formal ADI framework built on the principles of Self-Sovereign Identity to create a system that is user-centric, portable, verifiable, and private by design.

4.1 Formal Definition

An Academic Digital Identity (ADI) is an authoritative, lifelong digital persona representing an individual's verified academic achievements, credentials, and affiliations. It is designed to be portable across institutions and borders, persist throughout a scholar's life, and remain under the exclusive control of the individual, enabling secure, privacy-preserving, and trustworthy academic interactions in a digital world.

4.2 Core Principles and Elements

The ADI framework is predicated on the following SSI principles and technical elements:

- **User Sovereignty and Control**: The scholar retains ultimate control and ownership over their ADI. They determine with precision the specific information to disseminate, the individuals with whom it shall be shared, and the duration of such dissemination. This is enabled by a personal digital wallet, a user-controlled application for storing and managing credentials [22].
- **Persistent Identifier (PID):** The ADI is anchored by a Decentralized Identifier (DID), a unique, globally resolvable identifier created and controlled by the user, not assigned by a central authority [23].
- **Verifiable Credentials (VCs):** Academic achievements are represented as Verifiable Credentials, aW3C open standard for digital credentials that are cryptographically signed, tamper-evident, and instantly verifiable without contacting the original issuer [24], [25], [26].
- **Interoperability:** By using open standards like DIDs and VCs, the ADI is natively interoperable, allowing for seamless recognition of qualifications across diverse global systems [27], [28].

Minimal Disclosure and Privacy: The framework enables selective disclosure, allowing a scholar to prove a specific attribute (e.g., "holds a PhD") without revealing unnecessary underlying data, thus protecting privacy [29], [30].

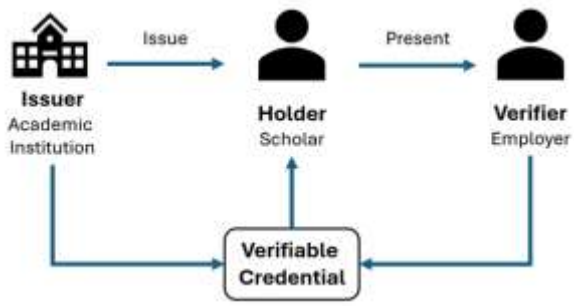

Figure 3 The Academic Digital Identity (ADI) based on SSI Model

4.3 Architectural Contrast: ADI vs. DigiLocker / APAAR

Error! Reference source not found. summarizes the fundamental architectural differences between the proposed ADI framework and current centralized models.

Table 1 Comparison between centralized ADAAR and SSI based ADI

Feature	DigiLocker / APAAR (Centralized)	Academic Digital Identity (SSI-based)
Architecture	Centralized. Data flows through government-managed servers (e.g., NAD, DigiLocker) [31].	Decentralized. Peer-to-peer interactions anchored on a distributed ledger [32].
Data Control	User-consented access, but ultimate control lies with the platform/government [19].	Absolute user control. Data is held in the user's private digital wallet [22].
Identifier	APAAR ID (linked to Aadhaar). Centrally assigned and managed [33].	Decentralized Identifier (DID). Created and controlled by the user [23].
Data Format	Platform-specific formats like signed PDF/XML [34].	W3C Verifiable Credentials (VCs). An open, interoperable standard [24].
Global Verification	Limited. Relies on bilateral agreements or bespoke integrations [19].	Natively interoperable. Any verifier worldwide can cryptographically check a VC [28].
Privacy	Relies on platform security and policy. Data aggregation is possible [20].	Privacy-by-design. User holds data. Selective disclosure protects privacy [30].
Trust Model	Trust in the government/platform as a central authority.	Trust in cryptography and a decentralized network of issuers and verifiers [35].

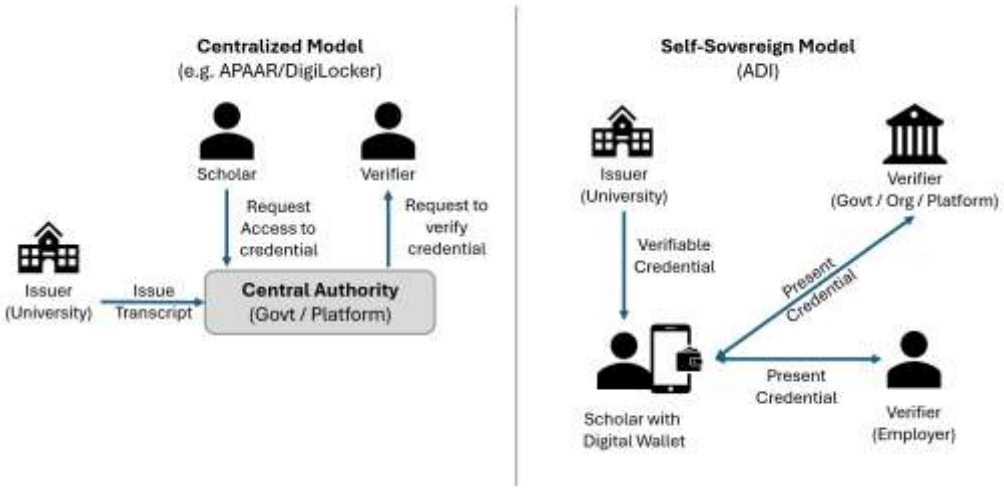

Figure 4 Architectural Comparison: Centralized vs Self-Sovereign Identity Model

V. DISCUSSION

The proposed ADI framework offers a transformative solution to the documented problems of the current academic identity landscape.

5.1 Resolving Documented Problems

By providing a unified, user-controlled identity, the ADI framework directly addresses the fragmentation that burdens academics. Its cryptographic verification capabilities enhance academic integrity and reduce dependency on institutional systems. Furthermore, its privacy-preserving features counter concerns about institutional surveillance and dataveillance by shifting control over personal data from platforms to the individual [10].

5.2 Implication for Stakeholders

- **For Scholars:** The ADI grants ownership over lifelong learning records, enhances privacy, and reduces administrative friction. Individuals can build comprehensive, persistent portfolios that transcend institutional and national boundaries.

- **For Institutions:** The framework streamlines verification processes, enhances academic integrity by making credential fraud significantly more difficult, and offers modern infrastructure for serving a global academic community.
- **For the Ecosystem:** The ADI creates a trusted, interoperable layer that facilitates credit transfer, hiring, and peer review, reducing friction in academic mobility and enabling new forms of collaboration.

5.3 Implementation Challenges and Future Research

The realization of an SSI-based ADI, while compelling, faces challenges. Technical complexity around key management and wallet usability requires significant digital literacy development. Robust, decentralized governance frameworks must be established to accredit institutional issuers and ensure legal recognition of cryptographic credentials. Future work should focus on empirical studies testing the usability of SSI wallets for academics, developing these governance models, and conducting pilot projects to test the cross-border interoperability of the ADI framework.

VI. CONCLUSION

This paper has conceptualized the Academic Digital Identity (ADI) as a specialized, user-centric, and verifiable framework designed to address the pervasive digitization and fragmentation within contemporary scholarly practice. Drawing on the principle of contextual specialization, we have argued that the academic domain warrants a dedicated digital identity beyond general-purpose national identifiers. The proposed ADI model, predicated on Self-Sovereign Identity (SSI) principles, offers a robust solution to the limitations of current centralized systems by empowering scholars with sovereign ownership over their academic data. By facilitating selective disclosure, ensuring worldwide interoperability via open standards, and incorporating robust privacy safeguards, the Academic Digital Identity (ADI) possesses the capacity to transform the methodologies employed in measuring scholarly impact, promoting collaborative efforts, and advancing academic careers. Ultimately, the ADI transcends a mere technical proposal; it represents a fundamental re-conceptualization of the dynamics between scholars and their intellectual outputs, consequently, redistributes the locus of control from institutional entities to individual academics, thus laying the foundation for a more transparent, trustworthy, and equitable global academic commons.

REFERENCES

[1] M. Weller, *The Digital Scholar: How Technology is Transforming Scholarly Practice*. London: Bloomsbury Academic, 2011.

[2] L. Deborah, M. Inger, and P. Thomson, Eds., *The Digital Academic*, 1st ed. Routledge, 2017. doi: 10.4324/9781315473611.

[3] "Global Networking on Secure Academic Credentials," in *Springer International Handbooks of Education*, Cham: Springer Nature Switzerland, 2024, pp. 1039–1061. doi: 10.1007/978-3-031-54144-5_178.

[4] A. Quintas-Mendes and A. Paiva, "Digital Presence and Online Identity among Digital Scholars: A Thematic Analysis," *Soc. Sci.*, vol. 12, no. 7, p. 379, June 2023, doi: 10.3390/socsci12070379.

[5] R. M. G. Marques, A. Lopes, and A. M. Magalhães, "Academic identities and higher education change: reviewing the evidence," *Educ. Res.*, vol. 66, no. 2, pp. 228–244, Apr. 2024, doi: 10.1080/00131881.2024.2334760.

[6] H. Strack *et al.*, "Digitization of (Higher) Education Processes: Innovations, Security and Standards," in *EPiC Series in Computing*, EasyChair, pp. 22–9. doi: 10.29007/rrg4.

[7] W. Suktam, S. Lapchit, J. Supsin, S. Sonwa, and C. Suthamdee, "Blockchain in Education: Transforming Learning, Credentialing, and Academic Data Management," *J. Educ. Learn. Rev.*, vol. 1, no. 6, pp. 37–46, Oct. 2024, doi: 10.60027/jelr.2024.739.

[8] P. Hiradhar and J. Gray, "From a social digital identity to an academic digital identity: Introducing ePortfolios in English language enhancement courses," *Can. J. Learn. Technol. Rev. Can. L'apprentissage Technol.*, vol. 34, no. 3, Apr. 2009, doi: 10.21432/t2q30j.

[9] B.-A. Andrea, N.-T. Miguel, G.-R. Frank, C. Ramiro, and B.-P. Andrés, "Visibility of Scientific Production and Digital Identity of Researchers through Digital Technologies," *Educ. Sci.*, vol. 12, no. 12, p. 926, Dec. 2022, doi: 10.3390/educsci12120926.

[10] R. Burrows, "Living with the H-Index? Metric Assemblages in the Contemporary Academy," *Sociol. Rev.*, vol. 60, no. 2, pp. 355–372, May 2012, doi: 10.1111/j.1467-954X.2012.02077.x.

[11] A. Inamorato Dos Santos, E. Chinkes, M. A. G. Carvalho, C. M. V. Solórzano, and L. S. Marroni, "The digital competence of academics in higher education: is the glass half empty or half full?," *Int. J. Educ. Technol. High. Educ.*, vol. 20, no. 1, Feb. 2023, doi: 10.1186/s41239-022-00376-0.

[12] D. Berbecaru, A. Lioy, and C. Cameroni, "Providing digital identity and academic attributes through European eID infrastructures: Results achieved, limitations, and future steps," *Softw. Pract. Exp.*, vol. 49, no. 11, pp. 1643–1662, Nov. 2019, doi: 10.1002/spe.2738.

[13] S. Seema, "Apaar ID: □□□□□ □□□ □□□ 31.56 □□□□□ □□□□□□□ □□ □□□□ □□□□□ □□□□□□ □□□□□; □□□□□ □□□□□□ □□□□□, □□□□□ □□□□ □□□□," *Amarujala*, July 30, 2025. [Online]. Available: https://www.amarujala.com/education/apaar-id-315-6-million-students-in-india-get-unique-digital-identity-uttar-pradesh-leads-bengal-lags-behind-2025-07-30

[14] "A Document Walletto Empower Citizens." Ministry of Electronics & Information Technology. [Online]. Available: https://egovstandards.gov.in/sites/default/files/2023-05/DigiLocker%20Deck.pdf

[15] U. Rao and G. W. Greenleaf, "Subverting ID from above and below: The uncertain shaping of India's new instrument of e-governance," *Surveill. Soc.*, vol. 11, no. 3, pp. 287–300, Dec. 2013, doi: 10.24908/ss.v11i3.4496.

[16] U. Rao and V. Nair, "Aadhaar: Governing with Biometrics," *South Asia J. South Asian Stud.*, vol. 42, no. 3, pp. 469–481, May 2019, doi: 10.1080/00856401.2019.1595343.

[17] P. Varma, "Building an Open Identity Platform for India," in *2015 Asia-Pacific Software Engineering Conference (APSEC)*, New Delhi: IEEE, Dec. 2015, pp. 3–3. doi: 10.1109/apsec.2015.63.

[18] "Shri Dharmendra Pradhan inaugurates National Conference on APAAR: One Nation One Student ID Card," Press Information B, Delhi, Press Release 2005706, Feb. 2024. [Online]. Available: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2005706

[19] "DigiLocker vs. Blockchain-based Credentials: A Comparative Analysis." [Online]. Available: https://www.truscholar.io/blog/digilocker-vs-blockchain-based-credentials-a-comparative-analysis
[20] Anand Upadhyay, "Analyzing the Impact of Digital Literacy and Security on DigiLocker Adoption in India," *J. Inform. Educ. Res.*, vol. 5, no. 2, May 2025, doi: 10.52783/jier.v5i2.2833.
[21] D. Kotis and C. Rath, "Strengthening our defenses: The role of the health-system pharmacist in cybersecurity management," *JACCP J. Am. Coll. Clin. Pharm.*, vol. 4, no. 6, pp. 662–663, June 2021, doi: 10.1002/jac5.1463.
[22] M. Korir, S. Parkin, and P. Dunphy, "An Empirical Study of a Decentralized Identity Wallet: Usability, Security, and Perspectives on User Control," in *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, Boston: USENIX, 2022, pp. 195–211. [Online]. Available: https://www.semanticscholar.org/paper/An-Empirical-Study-of-a-Decentralized-Identity-and-Korir-Parkin/f088153af0186a17a106601ce1aabe138c1a33f6
[23] W. Chan, K. Gai, J. Yu, and L. Zhu, "Blockchain-Assisted Self-Sovereign Identities on Education: A Survey," *Blockchains*, vol. 3, no. 1, p. 3, Feb. 2025, doi: 10.3390/blockchains3010003.
[24] M. Sporny, D. Longley, D. Chadwick, and I. Herman, *Verifiable Credentials Data Model v2.0*, Mar. 20, 2025. [Online]. Available: https://www.w3.org/TR/vc-data-model-2.0/
[25] P. Herbke and H. Yildiz, "ELMO2EDS: Transforming Educational Credentials into Self-Sovereign Identity Paradigm," in *2022 20th International Conference on Information Technology Based Higher Education and Training (ITHET)*, Antalya, Turkey: IEEE, Nov. 2022, pp. 1–7. doi: 10.1109/ithet56107.2022.10031276.
[26] E. Tan, E. Lerouge, J. Du Caju, and D. Du Seuil, "Verification of Education Credentials on European Blockchain Services Infrastructure (EBSI): Action Research in a Cross-Border Use Case between Belgium and Italy," *Big Data Cogn. Comput.*, vol. 7, no. 2, p. 79, Apr. 2023, doi: 10.3390/bdcc7020079.
[27] N. Chotikakamthorn, A. Mi San, and C. Sathitwiriyawong, "On-Chain Verifiable Credential with Applications in Education," *ECTI Trans. Comput. Inf. Technol. ECTI-CIT*, vol. 18, no. 3, pp. 342–355, July 2024, doi: 10.37936/ecti-cit.2024183.256091.
[28] G. Bernstein, D. Burnett, and D. Chadwick, *Verifiable Credentials Overview*. 2025. [Online]. Available: https://www.w3.org/TR/vc-overview/
[29] R. R. Sekar, A. Masna, S. Sharma, A. Abraham, and P. R. Pagilla, "Decentralized Identity and Access Management (IAM) Using Blockchain," in *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)*, Gurugram, India: IEEE, May 2024, pp. 1–6. doi: 10.1109/iscs61804.2024.10581159.
[30] X. Yang and W. Li, "A zero-knowledge-proof-based digital identity management scheme in blockchain," *Comput. Secur.*, vol. 99, p. 102050, Dec. 2020, doi: 10.1016/j.cose.2020.102050.
[31] "DigiLocker Security Architecture." Government of India. Accessed: Aug. 01, 2025. [Online]. Available: https://www.digilocker.gov.in/web/security-architecture
[32] Md. R. Ahmed, A. K. M. M. Islam, S. Shatabda, and S. Islam, "Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey," *IEEE Access*, vol. 10, pp. 113436–113481, 2022, doi: 10.1109/ACCESS.2022.3216643.
[33] H. M. Naveen, "ESTABLISHMENT AND OPERATION OFACADEMIC BANK OF CREDITS (ABC) INHIGHER EDUCATION," *IJEAST*, vol. 6, no. 5, pp. 166–169, Sept. 2021.
[34] "Technology Overview - The Engine Behind DigiLocker." Government of India. [Online]. Available: https://www.digilocker.gov.in/web/technology
[35] Y. Bai, H. Lei, S. Li, H. Gao, J. Li, and L. Li, "Decentralized and Self-Sovereign Identity in the Era of Blockchain: A Survey," in *2022 IEEE International Conference on Blockchain (Blockchain)*, Espoo, Finland: IEEE, Aug. 2022, pp. 500–507. doi: 10.1109/Blockchain55522.2022.00077.