2026 Volume: 02 Issue: 05 www.ijrpa.com ISSN 2456-9995 Research Article

International Journal Research Publication Analysis

Page: 01-12

DECENTRALIZED DIGITAL IDENTITY AND VERIFIABLE CREDENTIALS IN SEMANTIC WEB ARCHITECTURES

Ayush[1], Nikita Malik[2*]

[1]Student, Dept. of Computer Applications, Maharaja Surajmal Institute, New Delhi

[*2]Assistant Professor, Dept. of Computer Applications, Maharaja Surajmal Institute, New Delhi.

Article Received: 25 March 2026
Article Revised: 15 April 2026
Published on: 05 May 2026

***Corresponding Author: Nikita Malik**
Assistant Professor, Dept. of Computer Applications, Maharaja Surajmal Institute, New Delhi.

DOI: https://doi-doi.org/101555/ijrpa.5486

ABSTRACT

Single points of failure, large-scale data breaches, and excessive data exposure are some of the critical vulnerabilities that have been introduced by the proliferation of centralized digital identity systems. Over 422 million personal records were stolen across the globe in 2022, and it is necessary to discover stronger options [1]. The current paper discusses Decentralized Digital Identity using Decentralized Identifiers (DIDS) and Verifiable Credentials (VCs) founded on Semantic Web standards as one of the solutions to such problems. The paper is founded on the W3C specifications of both the DID Core and the Verifiable Credentials Data Model v2.0, and discusses both the overall credential lifecycle and the trust architecture of issuers, holders, and verifiers, and the use of RDF, JSON-LD, and SPARQL to achieve semantic interoperability of heterogeneous systems. A good example of how educational credentials can be used is provided, where educational institutions in India can employ tamper-evident cryptographically signed credentials which can be authenticated by employers without the need of contacting the issuer. The comparative analysis is centralized, federated, and decentralized identity and SSI has advantages of user control, privacy of selective disclosure and regulatory consistency with the laws such as the DPDP Act in India and the GDPR in the EU. The most recent issues such as blockchain scalability, metadata privacy and lack of usability are addressed, as well as future research directions such as quantum-resistant cryptography and AI-assisted verification. There is a claim that this architecture is a viable and standards-compliant way to user-centric, trust-minimized digital identity management.

KEYWORDS: Decentralized Identifiers (DID); Verifiable Credentials (VC); Self-Sovereign Identity (SSI); Semantic Web; JSON-LD; Blockchain.

1. INTRODUCTION

1.1 Motivation and Problem Statement

The existing digital identity system is largely established on centralized systems, owned and managed by governments or major service providers. These architectures expose the users to high-risk situations. The Identity Theft Resource Center reported that in data breaches alone 422 million individual records were compromised in 2022 alone, and this figure is increasing [1]. The problem of document forgery is acute, especially in the developing economies where the checks and balances of academic and professional qualifications are not always conducted and are frequently postponed [2]. Moreover, the current paradigm forces consumers to part with unequal portions of personal data in order to enjoy even the most basic digital services, posing systemic privacy issues [3].

1.2 Limitations of Centralized Identity Systems

The centralized identity systems have a number of architectural flaws, which cause underlying issues [4]. To begin with, they are single points of failure: in case of a disruption of a central server, the whole authentication service is inaccessible to everyone. Second, central databases hosting user data significantly compromise the risk of mass and simultaneous data leakage of millions of users [5]. Third, users are forced to provide their complete identity profile on each transaction, rather than cherry-picking and disclosing only those attributes that are relevant to the interaction [6]. Fourth, the authentication latency and infrastructure capacity of dense areas becomes a bottleneck with the user number [7]. Fifth, centralized architectures result in structural stumbling block among identities of different organizations in the area of communication resulting in identity silos in isolation [8].\

1.3 The Need for Decentralized Solutions

D-ID Systems provide the user with sovereignty over their Verifiable Credentials and, therefore, with whom they share their information. It is the nature of the Self-Sovereign Identity (SSI) model where no centralized intermediaries are involved, and all the data sovereignty is located on the owner of the credential in its fullness [5]. The practical advantages of the SSI model are many: the model is less susceptible to identity theft, users can choose to disclose selectively, and the validation of qualification is quick and independent, without institutional intermediaries. This is more so true in competitive

employment market such as in India where delays in credential verification leads to massive delays among job seekers and employers [10].

1.4 Objectives and Paper Organization

This paper discusses Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) and how Semantic Web technologies enable their interoperability. The paper discusses: the background background on the evolution of digital identities (Section 2); the technical architecture of DIDs (Section 3); the verifiable credentials data model and lifecycle (Section 4); semantic interoperability mechanisms (Section 5); system architecture and an educational use case (Section 6); a results and comparative analysis (Section 7); current challenges and future directions (Section 8); and a concluding summary (Section 9).

2. BACKGROUND AND FOUNDATIONAL CONCEPTS

2.1 Digital Identity Evolution

Several paradigms have been witnessed in digital identity system development. The first systems used usernames and passwords combination which offered a very weak and fragile authentication mechanism. Federated Identity Management was made possible by the creation of Single Sign-On (SSO) protocols, based on standardized identifiable frameworks like OAuth 2.0 and SAML, with the help of which a single user ID can be used to log in to various systems. Despite this facilitating user experience, it still relied on centralized trust architectures with a similar attack surface [4]. The next step is Self-Sovereign Identity, where the metadata of the credentials is stored in a tamper-evident, decentralized registry, to ensure that it is not required to be reliant on a central identity provider, relying on Distributed Ledger Technology (DLT) [5][13]. Standardization has played a critical part in W3C, and this has assisted in bringing these experimental systems to interoperable, production-ready implementations [9].

2.2 Semantic Web Fundamentals

The Semantic Web as conceived by Berners-Lee et al. is intended to allow computers to process and reason over the contents of the data, not just index it. It has a fundamental framework that is built based on the Resource Description Framework (RDF) that represents knowledge in terms of triples subject-predicate-object. The web ontology language (OWL) extends RDF to allow more rational connections between concepts. RDF data has a query language named SPARQL, which is capable of the same type of searches as the SQL in relational databases. JSON-LD (JavaScript Object Notation of Linked Data) is a serialization

of RDF, which is simple to manipulate by a programmer, and can be combined with web app stacks [9][11]. The framework offers a shared semantic layer to decentralized identity systems; in other words, information interchanged among heterogeneous systems is interpreted in the same way.

2.3 W3C Standards Overview

The standardization of open infrastructure of decentralized identity has been greatly influenced by the World Wide Web Consortium (W3C). In 2022, W3C DID Core was made a Recommendation [2], and continues to be a working group draft. In 2025, W3C published the Verifiable Credentials Data Model v2.0 that added additional privacy controls, better interoperability with JSON-LD and provided new cryptographic proof formats [9]. The combination of these standards allows verifiable credentials to be validated in a secure manner across a wide variety of systems whilst eliminating a single point of trust dependency.

3. DECENTRALIZED IDENTIFIERS

3.1 DID Architecture

A Decentralized Identifier is a unique identifier around the world that is persistent and does not need a central registration authority to be initiated or managed [2][12]. A DID is in canonical form: did:method:unique-part. The method element describes the technical mechanism through which the DID is generated, read, modified and deactivated. Approaches can include web-hosted (did:web) or blockchain-made registries (did:ethr, did:ion). The essential characteristic of a DID is that only the controller can modify or revoke the DID with the help of the respective cryptographic private key [4].

3.2 DID Documents

All DIDs resolve to a related DID Document, which is normally in the format of JSON or JSON-LD. The DID Document includes: the public keys to authenticate the DID controller; the verification relationships (e.g., authentication, key agreement); and optional service endpoints, e.g., secure messaging endpoints or credential status registries [2]. The document under consideration lies fully in the hands of the DID subject and can be changed only in accordance with the rules that are peculiar to the method. This is a stark contrast to profile information stored by centralized identity providers, not under any meaningful control of the users.

3.3 DID Resolution

The dereferencing of a DID string, to access the associated DID Document, is known as DID resolution. Various DID approaches are different ways of resolving. The did:web approach maps a DID string to a URL, which is under the control of the DID subject, providing simplicity, but with a dependency on the web server staying online [3]. The did:ethr approach grounds the DID in the Ethereum blockchain and is more strongly decentralized at the expense of the gas charge and transaction latency [6]. Universal Resolvers as defined by the Decentralized Identity Foundation (DIF) allow one interface to resolve DIDs using a variety of means [7].

4. VERIFIABLE CREDENTIALS

4.1 Verifiable Credential Data Model

A Verifiable Credential (VC) is a cryptographically signed digital credential claim that is made by an issuer concerning a credential subject [9]. A credential, as defined by the W3C VC Data Model v2.0, has the following elements: a context field indicating the vocabulary used (@context); a type field indicating the type of credential; a credentialSubject object, which holds the claims; an issuer field indicating the issuer with a DID; an issuanceDate and optional expirationDate fields; and a cryptographic proof block that indicates authenticity. This data is always represented in a serial form using the JSON-LD and it allows machine-readable interoperability between systems [9][11].

4.2 Credential Lifecycle

Verifiable Credential lifecycle comprises three main stages. During the issuance process, the issuer (e.g. a university) gathers the credential information, cryptographically signs it with its associated DID-related private key, and sends it to the recipient. The credential holder stores the credential in a digital identity wallet. During the presentation phase, the holder generates a Verifiable Presentation (VP), and it can include one or more credentials and can disclose certain attributes selectively. The verification phase allows the verifier to independently solve the issuer DID, recover the issuer corresponding public key on the DID Document and cryptographically verify the signature on the credential without communicating with the issuer directly [3][10]. This is explained in figure 1.

Figure 1: Verifiable Credential Lifecycle (Issuance → Storage → Presentation → Verification).

4.3 Privacy Features

The VC model has a number of privacy-saving mechanisms. Verifiable Presentations Verifiable Presentations are a type of selective disclosure that enables holders to disclose only the particular claims needed to accomplish a certain interaction, such as demonstrating degree completion without disclosing the grade transcript [6]. Zero-Knowledge Proofs (ZKPs) enable their owners to demonstrate statements about their properties, e.g., that they are older than some age, without disclosing the data value [4]. The VC Data Model v2.0 also provided better unlinkability, which now was much more difficult to correlate the usage of similar credentials across one or more verification events [9]. All these features offer a huge privacy enhancement in comparison to centralized credential storage.

5. SEMANTIC INTEROPERABILITY IN DECENTRALIZED IDENTITY

5.1 The Role of Standardized Vocabularies

Any cross-organizational identity ecosystem is based on semantic interoperability, which involves the capacity of different systems to correctly process shared data [8]. JSON-LD and RDF allow different systems to have a common set of definitions of terms like degree, expirationDate, or credentialSubject. In the absence of a shared semantic system, a credential presented by one system, can have completely different implications when presented to a different system. Schema.org offers standard terms of common objects such as people, organizations and educational qualifications, and domain ontologies enable jurisdictions to provide specialized credential format formats as per local demand [9].

5.2 Cross-Platform Credential Compatibility

With a decentralized identity ecosystem, verifiers can be faced with credentials issued by entities in completely distinct jurisdictions based on different technical stacks. The principles of Linked Data guarantee that a verifier can dereference an external context-URL carried in a

credential to get the vocabulary definition and experience consistent interpretation without the bilateral agreement in advance [2][9]. In the case of the Indian educational system this would imply that a degree provided by an institution accredited by the University Grants Commission (UGC) anywhere in the globe would be verified by either of the employers as long as they both subscribe to the W3C VC and DID standards. The similar querying of RDF-encoded credential data with the help of SPARQL also facilitates policy-driven, automated verification processes [8].

6. SYSTEM ARCHITECTURE AND EDUCATIONAL USE CASE

6.1 Trust Architecture

The decentralized identity architecture is structured around three main roles: the Issuer, the Holder, and the Verifier, and is often referred to as the Trust Triangle [5][7]. The Issuer signs the credential and signs it with the DID-related private key. The Holder is provided with credentials in a digital wallet and the choice of whom to share with and when is an agency of the Holder. The Verifier authenticates credentials by determining the DID of the issuer and verifying the cryptographic signature with the public key included with the DID Document, and does not need to interact with the issuer. Under this hierarchy is a Verifiable Data Registry (VDR) that is generally a blockchain or distributed registry, an authoritative, evidenced-tampered repository of DID Documents. The cryptographic layer provides provable trust; the semantic layer that claims can be understood in systems. This architecture is shown in figure 2.

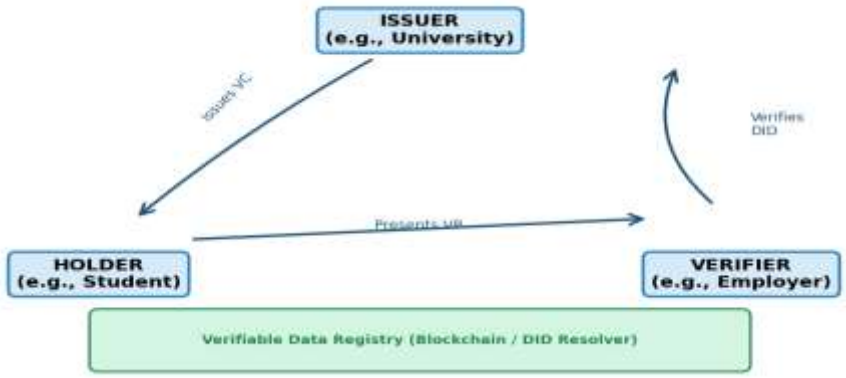

Figure 2: The Decentralized Identity Triangle with the relationships between Issuer, Holder and Verifier.

6.2 Educational Credential Use Case

An Indian university giving a verifiable degree to a graduating student is a real-world example of what can be done to base this architecture on. The steps followed are as follows: (1) The Issuer is the university that collects the credential with the name of the student, degree, programme, year and result. This credential is encoded in JSON-LD and cryptographically signed with the help of the university private key related to its registered DID. (2) The signed credential is sent to the student and the identity wallet application stores the credential in a wallet. (3) At the time when the student applies to a job, he or she develops a Verifiable Presentation in his or her wallet, and only the information about the degree completion is selectively disclosed with no disclosure of grades and other personal data than what is required. (4) The Verifier, which is the employer, solves the DID of the university through Universal Resolver, retrieves the public key of the DID Document and independently verifies the signature of the credential. The whole process of verification is accomplished in a few seconds and does not involve the personal communication with the university.

This addresses three nagging issues with the existing system of Indian employment credentialing: the submission of blurred document photos which can be forged with trivial ease; the time lag created by universities in responding to employer requests; and the threat of fake degree certificates, which still cost reputational and financial damage not only to employers but also to honest degree holders [10].

7. RESULTS AND ANALYSIS

7.1 Comparative Analysis of Identity Paradigms

This paper has performed a comparative analysis of the SSI-based decentralized identity model against existing identity models in eight criteria, namely, user control, a single point of failure, the risk of data breaches, interoperability, selective disclosure, scalability, verification mode, and regulatory alignment. The findings are summarized as in table 1.

Table 1: Comparative Analysis of Identity System Paradigms.

Criterion	Centralized Identity	Federated Identity	SSI / Decentralized
User Control	None (provider-owned)	Partial (IdP-managed)	Full (user-owned)
Single Point of Failure	Yes	Partial	No
Data Breach Risk	High	Medium	Low
Interoperability	Low (silo-based)	Moderate (federation)	High (W3C standards)
Privacy (Selective Dis.	Not supported	Limited	Supported (ZKP)
Scalability	Limited by server	Moderate	High (distributed)
Credential Verification	Requires issuer online	Requires IdP online	Offline possible
Regulatory Alignment	Complex	Complex	Designed for GDPR/DPDP

7.2 Architectural Contribution

As can be seen in the analysis provided in Table 1, decentralized identity systems based on SSI consistently outperform centralized and federated identity systems in most of the criteria considered. The proposed approach has made the following significant contributions to architecture: (i) Complete user control over credential data, in which cryptographic ownership of DID can be proven, and (ii) privacy-preserving selective disclosure and attribute proofs based on ZKP, which are not structurally present in either centralized or federated model; (iii) Semantic interoperability, where credential portability across institutional or jurisdictional boundaries is achievable without prior bilateral agreement; and (iv) The ability to verify offline, which is made possible by resolving cryptographic signatures against pre-fetched DID Documents, and does not require real-time participation of the issuer [4][7].

7.3 Applicability to the Indian Context

The model of a decentralized identity has quantifiable benefits within the framework of the concrete context of India. The Digital Personal Data Protection (DPDP) Act 2023 of the country requires that personal data processing is carried out with explicit, limited-purpose consent, which is precisely the selective disclosure system of Verifiable Credentials [8]. Moreover, the high rates of document forgery in educational and professional qualifications in India also provide a good practical incentive towards cryptographically verifiable, tamper-evident alternatives [2]. The empirical validation that institutions in education, healthcare and

government services would need to develop the public trust and facilitated a wider adoption of the SSI model would be supplied by pilot implementations.

8. CHALLENGES AND FUTURE DIRECTIONS

8.1 Current Obstacles

Although there are some architectural benefits of decentralized identity, a number of practical issues still exist. To start with, despite the fact that selective disclosure reduces most of the privacy risks, correlation of user behavior across interactions can still be made by metadata leakage due to credential use patterns [6]. Second, mainstream blockchain services are not scalable and cost-effective enough to support mass-market identity applications, and transaction costs and confirmation times present a viable obstacle [3][12]. Third, digital identity wallets and DID tooling are still technically tricky to non-expert users, which is a great usability hurdle to widespread adoption [8]. Fourth, the regulatory environment is still in pieces; whereas both the DPDP Act in India and the GDPR in the EU focus on data minimization and user consent, they have different technical demands, which makes cross-jurisdictional implementation challenging [1][9].

8.2 Future Research Directions

These issues can be solved with the help of a number of research directions. Using Artificial Intelligence to verify claims automatically and detect anomalous presentation may increase the level of verification and fraud resistance. The threat of quantum computing is rising; therefore, standardization and development of quantum-resistant cryptographic algorithms, including those currently being standardized by NIST, are an urgent priority to long-term DID and VC security [4]. The current gap to usability may be reduced through the study of hybrid identity models, which offer a simpler user experience over an actually decentralized backend. Finally, real pilot application in Indian schools and government service would give results of the empirical data that would be incorporated to enhance the technical standards, as well as the regulatory frameworks of SSI [10][13].

9. CONCLUSION

In this paper, I have addressed Decentralized Digital Identity and Verifiable Credentials as a framework that is technically foundational and based on standards to the organizational problems of centralized identity paradigms. The architecture proposed, using W3C-standardized DID, Verifiable Credentials Data Model v2.0, and Semantic Web technologies, including JSON-LD and RDF, offers user-controlled privacy-preserving, and interoperable

identity management, and is compliant with the current data protection legislation [1][9]. The comparative analysis reveals clear advantages on the user sovereignty, privacy, interoperability and scalability dimensions as compared to centralized and federated models [5][8]. The case of educational credential shows that the use case is applicable in the near future, i.e. in the Indian context, document frauds and document verification delays entail real economic costs. Despite the fact that scalability, usability, and regulatory harmonization still are a problem, the ongoing work on standardization by W3C, and the research of quantum-resistant cryptography and AI-assisted verification are all good signs that there is a viable path to mainstream use. Decentralized identity is not merely a partial solution, but a systemic change in the architecture to a future where there is few or no trust, and user-sovereign digital identity.

REFERENCES

1. Identity Theft Resource Center (ITRC). (2022). 2022 Annual Data Breach Report. San Diego: ITRC. Available: https://www.idtheftcenter.org/publication/2022-annual-data-breach-report/
2. World Wide Web Consortium (W3C). (2022). Decentralized Identifiers (DIDs) v1.0: Core Architecture, Data Model, and Representations. W3C Recommendation. Available: https://www.w3.org/TR/did-core/
3. Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. Computer Science Review, 30, 80–86. https://doi.org/10.1016/j.cosrev.2018.10.002
4. Abraham, A., More, S., Rabensteiner, C., & Hörandner, F. (2020). Revocable and Offline-Verifiable Self-Sovereign Identities. In Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 1020–1027. IEEE. https://doi.org/10.1109/TrustCom50675.2020.00134
5. Ferdous, M. S., Chowdhury, F., & Alassafi, M. O. (2019). In Search of Self-Sovereign Identity Leveraging Blockchain Technology. IEEE Access, 7, 103059–103079. https://doi.org/10.1109/ACCESS.2019.2931173
6. Naik, N., & Jenkins, P. (2020). Self-Sovereign Identity Specifications: Govern Your Identity Through Your Digital Wallet Using Blockchain Technology. In Proceedings of the 2020 IEEE 8th International Conference on Intelligent Systems (IS). IEEE. https://doi.org/10.1109/IS48319.2020.9199940

7. Brunner, C., Gallersdörfer, U., Knirsch, F., Engel, D., & Matthes, F. (2020). DID and VC: Untangling Decentralized Identifiers and Verifiable Credentials for the Web of Trust. In Proceedings of the 3rd International Conference on Blockchain Technology and Applications (ICBTA), pp. 61–66. ACM. https://doi.org/10.1145/3446983.3446992
8. Zwitter, A. J., Gstrein, O. J., & Yap, E. (2020). Digital Identity and the Blockchain: Universal Identity Management and the Concept of the "Self-Sovereign" Individual. Frontiers in Blockchain, 3, Article 26. https://doi.org/10.3389/fbloc.2020.00026
9. World Wide Web Consortium (W3C). (2025). Verifiable Credentials Data Model v2.0. W3C Recommendation. Available: https://www.w3.org/TR/vc-data-model-2.0/
10. Kaneriya, J., & Patel, H. (2023). A Secure and Privacy-Preserving Student Credential Verification System Using Blockchain Technology. International Journal of Information and Education Technology, 13(8). https://doi.org/10.18178/ijiet.2023.13.8.1900
11. Sporny, M., Longley, D., & Kellogg, G. (2020). JSON-LD 1.1: A JSON-based Serialization for Linked Data. W3C Recommendation. Available: https://www.w3.org/TR/json-ld11/
12. Mazzocca, C., Acar, A., Uluagac, S., Montanari, R., Bellavista, P., & Conti, M. (2025). A Survey on Decentralized Identifiers and Verifiable Credentials. IEEE Communications Surveys & Tutorials. https://doi.org/10.1109/COMST.2025.3543197
13. Tavares Aranha, H., Rodrigues, M., Ferreira, D., & Antunes, N. (2022). Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy. Sensors, 22(15), 5641. https://doi.org/10.3390/s22155641 [PMC9371034]