International Journal of Research in Engineering, Science and Management
Volume 9, Issue 7, July 2026
www.ijresm.com | E-ISSN: 2581-5792 | RESAIM Publishing | www.resaim.com

Decentralised Self-Sovereign Identity (SSI) for Secure Employee Credentialing and Fraud Prevention in AI-Driven Talent Acquisition: A Conceptual Framework and System Architecture

Sadaf Khan[1], Kajal Yadav[1], Soumya Batra[1*]
[1]*Faculty of Management and Commerce, SAM Global University, Raisen, India*

Abstract*: The rapid digitisation of human resource management (HRM) has accelerated the adoption of automated talent acquisition systems. However, this transition has also facilitated an unprecedented rise in curriculum vitae (CV) fraud, including credential falsification and employment history padding, which imposes severe financial and reputational liabilities on organisations. Traditional background screening processes are slow, costly, and heavily reliant on centralised third-party verification agencies. To address these challenges, this paper proposes a decentralised Self-Sovereign Identity (SSI) framework for secure employee credentialing and fraud prevention in talent acquisition. Adopting a conceptual framework and systems architecture methodology, and informed by a systematic analysis of 28 core research papers on blockchain, decentralised identity, and macro decentralised in HRM, we design a four-layer architecture. The proposed model successfully resolves the privacy-immutability paradox under the General Data Protection Regulation (GDPR) by storing Verifiable Credentials (VCs) and Decentralised Identifiers (DIDs) in user-controlled wallets while anchoring only cryptographic proofs on a public-permissioned blockchain. Our findings demonstrate that this framework eliminates resume fraud at the point of intake, reduces credential verification latency from weeks to seconds, and provides tamper-proof, structured data inputs that mitigate the 'garbage-in, garbage-out' risk in downstream machine learning applicant tracking systems. Ultimately, this research offers an operational roadmap for secure, privacy-preserving, and highly efficient digital recruitment ecosystems.

***Keywords*: Self-Sovereign Identity (SSI), Blockchain in HR, Credential Verification, Fraud Prevention, Talent Acquisition, Verifiable Credentials (VCs), Decentralised Identifiers (DIDs).**

1. Introduction

A. Background of the Study

The contemporary human resource management (HRM) landscape is undergoing a profound digital transformation, integrating advanced technologies into strategic organizational policies (Bondar, Organisational, 2025; Ping & Sakaki, 2026). Consequently, talent acquisition has evolved from manual, paper-based workflows into a digital, automated strategic function (Ping & Sakaki, 2026). Within this paradigm, organisations rely on automated organisation systems (ATS) and Artificial Intelligence (AI) to manage candidate profiles (Amanullah et al., 2026; Jimoh, 2026). By using machine learning models to parse resumes and rank applicants, organisations significantly reduce administrative overhead (Amanullah et al., 2026). However, these efficiency gains are heavily constrained by the authenticity and reliability of the underlying candidate data.

This reliance on digitized resume submissions has led to a critical vulnerability: the rising epidemic of CV fraud and credential padding (Chhetri, 2022; Saky et al., 2026). Studies indicate that many job applicants embellish qualifications, ranging from inflating employment durations to fabricating degrees and certifications (Saky et al., 2026). The ease of generating digital documents, combined with a lack of immediate verification channels, makes resume padding a low-risk strategy for organisations, with consequences including financial losses, compromised productivity, legal liabilities from negligent hiring, and reputational damage (Chhetri, 2022). Furthermore, discovering an unqualified hire forces a costly re-recruitment process. Therefore, establishing trust and data integrity at the talent intake phase has emerged as an urgent priority.

B. Problem Statement

To mitigate credential fraud, organisations traditionally perform background checks late in the hiring process. However, these traditional verification methods are slow and costly (Madhavi & Pande, 2025). Screening processes often take weeks as agents manually contact educational institutions, past employers, and registries, thereby increasing time-to-fill metrics. Additionally, relying on centralised third-party agencies incurs substantial fees per check, creating a significant financial burden at scale.

Beyond inefficiencies, centralised systems pose severe cybersecurity risks. Centralised candidate databases containing sensitive PII (e.g., identity numbers, transcripts, and salary histories) are high-value targets. Data breaches in centralised

*Corresponding author: soumyabatra123@gmail.com

HR systems and their centralised data repositories are increasingly frequent, exposing firms to regulatory penalties and reputational damage (Faruk & Khan, 2022).

To secure HR records, researchers propose integrating blockchain technology for its immutability and cryptographic tamper-evidence (Madhavi & Pande, 2025; Saky et al., 2026). However, this introduces the 'Immutability vs. Privacy Paradox' (Madanchiavs Taherdoost, 2026). Under GDPR Article 17 (the 'Right to be Forgotten'), individuals can request the deletion of their personal data. Because blockchain ledgers prevent modification, storing personal information on-chain directly violates data privacy laws. Consequently, a key challenge remains: how to construct a decentralised verification framework that ensures the integrity of candidate credentials without storing any PII on-chain, thereby achieving compliance with regulations.

C. Research Objectives

To address these critical research gaps, this study establishes a set of distinct research objectives focused on constructing a secure, privacy-compliant, and automated talent acquisition framework:

1. *Research Objective 1:* Design a multi-layered conceptual system architecture for employee credentialing that resolves the GDPR 'right to be forgotten' paradox. This architecture must separate sensitive personal data from cryptographic validation proofs by storing credentials off-chain while maintaining a decentralised, on-chain trust entity metadata.
2. *Research Objective 2:* Formulate a standardized data flow model based on the World Wide Web Consortium (W3C) Decentralised Identifiers (DIDs) and Verifiable Credentials (VCs) specifications, enabling secure, direct, and peer-to-peer exchange and verification of academic and employment records without relying on centralised third-party inter decentralised.
3. *Research Objective 3:* Outline the integration of the verifiable credential data flow with downstream corporate machine learning pipelines. This objective aims to demonstrate how structured, pre-verified JSON-LD credentials can be directly ingested by automated screening models, eliminating parsing errors, resolving the 'garbage-in, garbage-out' data quality problem, and establishing a baseline for bias-mitigated, objective candidate selection.

D. Scope of the Study

The scope of this study is strictly bounded to the recruitment intake, candidate sourcing, and credential validation phases of the talent acquisition lifecycle. Specifically, the proposed framework addresses the secure issuance, storage, presentation, and verification of core applicant credentials, which include academic degree certificates, past employment history records, and professional licensing details. By focusing on these high-risk areas where cretheal falsification is most prevalent, the study provides specialised, highly secure client verification at the point of application.

Conversely, the study excludes post-hire workforce management processes, such as employee onboarding workflows, internal training and skill development program tracking (Loidl et al., 2026), continuous performance management, internal talent promotion cycles (Jooss et al., 2019), payroll administration, and employee benefits optimization. While these inter optimisationions can benefit from decentralised records, their dadecentralised and operational requirements differ substantially from the external trust verification required during talent acquisition. Therefore, limiting the scope to the pre-employment intake phase ensures the proposed system architecture and data flows are optimized for high-volume, cross-organisational verification with maximum privacy controls.

2. Literature Review

A. Blockchain and decentralisation in Human Resource Decentralisation

In recent years, blockchain technology has emerged as a disruptive force across various administrative and strategic domains, with human resource management (HRM) representing a primary area of application. By design, a blockchain is a decentralised, distributed ledger that records transactions across a network of computers in a tamper-proof and immutable manner, governed by cryptographic consensus mechanisms. In the context of HR operations, blockchain provides a secure foundation for managing employee records, payroll, and recruitment, shifting the role of Human Resource Information Systems (HRIS) from simple clerical databases to strategic, trust-enabled business intelligence platforms (Batra & Sharma, 2022; Faruk & Khan, 2022). Scholars have emphasized that decentralisation can mitigate the vulnerabilities of traditional, centralised HR infrastructures, which are highly susceptible to single-point-of-failure cyberattacks and data tampering (Faruk & Khan, 2022). These traditional setups often build on centralised Intelligent Human Resource Information System (iHRIS) frameworks; while these functioned as useful decision-support tools, their reliance on centralised storage made them vulnerable to security threats and unauthorised access (Masum et al., 2018).

Earlier literature has explored various blockchain prototypes for credential verification. Chhetri (2022) identified that recruiters encounter frequent fraud and manual screening delays, and proposed a shared, decentralised verification database. Madhavi and Pande (2025) (along with Kumar and Kumar, 2025) implemented a person verification system using Ethereum smart contracts, enabling institutions to register credentials directly on-chain for instant verification. Additionally, Madanchian and Taherdoost (2026) developed a four-layer blockchain framework encompassing data, consensus, smart contract, and application layers to improve transparency and talent mobility.

Despite the security advantages demonstrated by these early implementations, they suffer from critical technical and

architectural limitations. Primarily, early models focused on direct on-chain storage of credential data or simple hashes linked to centralised databases, which fails to address the privacy requirements of modern data protection regulations (Madanchian & Taherdoost, 2026). Furthermore, deploying verification systems on public blockchains like Ethereum exposes organisations to prohibitive transaction (gas) fees and throughput bottlenecks, rendering them impractical for high-volume enterprise recruitment (Madhavi & Pande, 2025). Thus, while the literature establishes the theoretical feasibility of blockchain-enabled verification, it highlights a clear need for architectures that decouple the trust anchoring from the storage of sensitive personal data.

B. Self-Sovereign Identity (SSI) and the W3C DID/VC Standards

Self-Sovereign Identity (SSI) shifts digital identity from centralised and federated models to a user-centric paradigm. Traditional digital identities rely on third-party providers (e.g., Google, LinkedIn, or corporate directories) that store personal data in siloed databases. Conversely, SSI empowers individuals with ownership and autonomous control over their digital identity, eliminating external dependencies. Built upon principles of user control, access, transparency, persistence, and interoperability, SSI allows candidates to share credentials securely without leaving external digital footprints or exposing unnecessary personal details.

The operational foundation of SSI is governed by the cryptographic trust triangle, consisting of three main actors: the Issuer, the Holder, and the Verifier. The Issuer (such as a university or a former employer) is the authority that authenticates a set of attributes about an individual and issues a cryptographically signed digital credential. The Holder (the job seeker) receives the credential and stores it in a secure, private digital wallet on their personal device. When applying for a job, the Holder presents the credential to the Verifier (the recruiting organization), who can verify the cryptographic signature of the Issuer and ensure the credential has not been altered or revoked.

To ensure global interoperability, SSI frameworks adhere to the standards established by the World Wide Web Consortium (W3C). Key among these are the W3C Decentralised Identifiers (DIDs) v1.0 and Verifiable Credentials (VC) Data Model v1.1 recommendations (W3C, 2021, 2022). A DID is a new type of globally unique identifier that is cryptographically resolvable without a central registry (W3C, 2022). DIDs point to DID Documents, which reside on a Verifiable Data Registry (such as a blockchain) and contain cryptographic public keys and service endpoints. A Verifiable Credential is a machine-readable document containing structured claims (e.g., 'degree: Bachelor of Science') signed by the Issuer's private key (W3C, 2021). Through the use of public-key cryptography and advanced techniques like Zero-Knowledge Proofs (ZKPs) or selective disclosure, SSI enables candidates to present only the minimum required information (e.g., proving they possess a Master's degree without revealing their GPA or specific graduation year). This capability directly addresses the data minimization principles mandated by modern privacy regulations.

C. Artificial Intelligence and Machine Learning in Talent Acquisition

Parallel to the development of blockchain, the integration of Artificial Intelligence (AI) and Machine Learning (ML) has rapidly transformed the recruiting landscape. Organisations deploy AI/ML systems to automate high-volume talent sourcing, screen applications, match candidates to job specifications, and even predict post-hire performance and turnover (Zhai et al., 2024; Koştı & Kayadibi, 2025; Sakib & Islam, 2026). Systematic reviews indicate that AI-driven tools can process large datasets at speeds unattainable by human recruiters, utilizing machine learning algorithms such as Random Forests, Support Vector Machines (SVM), and XGBoost to classify candidate profiles (Căvescu & Popescu, 2025; Kovac et al., 2025; Amanullah et al., 2026). Natural Language Processing (NLP) models are also widely deployed to parse unstructured resume text, extracting skills, educational backgrounds, and employment history to match candidates with open roles (Suárez Pizzarello et al., 2026; Jimoh, 2026). This is supported by Vrontis et al. (2021), who conducted a comprehensive systematic review of advanced technologies, including robotics and AI, highlighting how their organizational adoption impacts employee trust and workflow structures.

However, the efficacy of AI/ML systems in recruitment is severely hindered by the 'Garbage In, Garbage Out' (GIGO) phenomenon, a fundamental limitation in algorithmic decision-making (Cheng & Hackett, 2021). Traditional candidate profiles and resumes consist of self-reported, unstructured text. Because this input data is unverified, ML models frequently ingest inaccurate, inflated, or completely fabricated information (Cheng & Hackett, 2021). This lack of data integrity compromises the predictive accuracy of the models, leading to suboptimal hiring decisions.

Refining unstructured PDF or Word documents requires complex NLP and Optical Character Recognition (OCR) engines, which are prone to format parsing errors, misclassification, and data loss. Non-standard resume designs, creative layouts, or table structures often lead to machine learning models misinterpreting candidate qualifications, thereby unfairly penalizing qualified candidates (Budhwar et al., 2022; Suárez Pizzarello et al., 2026). Consequently, there is a pressing need for a standardized, machine-readable, and cryptographically verified data format at the input stage. Integrating SSI-based Verifiable Credentials solves the GIGO problem by providing structured, pre-verified JSON-LD datasets, enabling ML screening engines to operate on 100% authentic inputs without the need for error-prone semantic parsing.

Indeed, as noted by Kovac et al. (2025) and Abadi and Outmane (2026), AI adoption is often hindered by tensions between control and autonomy, alongside difficulties in quantifying the return on investment (ROI) of predictive models. Traditional setups require complex data engineering pipelines to clean and normalize resume data before model

ingestion (Peeters et al., 2020; Chalutz Ben-Gal, 2019). This pre-processing is resource-intensive and introduces additional bias. Transitioning from unstructured resumes to verified credentials eliminates this costly pre-processing phase, improving the operational ROI of AI-driven talent systems (Chalutz Ben-Gal, 2019).

D. Ethical, Regulatory, and Privacy Challenges

The rapid integration of AI and decentralised databases in HR operations has sparked significant ethical, regulatory, and privacy concerns. At the forefront of regulatory compliance is the European Union's General Data Protection Regulation (GDPR), which imposes strict mandates on how personal data is processed, stored, and deleted. Under GDPR Article 17, individuals possess the right to erasure ('right to be forgotten'), requiring organisations to delete their PII upon request. Traditional blockchain-based HR systems, which write transactions directly to an immutable ledger, face severe compliance issues since on-chain data cannot be deleted (Madanchian & Taherdoost, 2026). Thus, designing systems that separate the validation ledger from actual identity data is crucial to resolving this regulatory barrier.

In addition to data privacy, algorithmic bias represents a major ethical challenge in digital recruitment. Cheng and Hackett (2021) argue that machine learning models trained on historical hiring data often inherit and amplify human biases, relying on heuristic correlations that penalize minority groups, women, or older candidates. Without clean, objective input data and transparent algorithmic rules, automated screening systems can codify historical inequalities and systemic discrimination (Cheng & Hackett, 2021; Patnaik, 2026). This issue is central to the human-centred agenda in HR technology advocated by Cappelli and Social Policy researchers (Cappelli & Rogovsky, 2023), who emphasize that AI systems must be designed to respect worker rights, promote equity, and maintain human oversight.

Candidate trust and system acceptance are heavily dependent on these ethical considerations. Using the Technology Acceptance Model (TAM), Obizue (2026) demonstrated that HR professionals and job applicants are hesitant to adopt AI-driven screening systems due to perceived opacity and potential unfairness. Ethical AI frameworks, as highlighted by Agwu (2026) and Patnaik (2026), must therefore incorporate mechanisms that guarantee input data authenticity and algorithmic transparency. By utilizing SSI, candidate credentials are pre-verified and structured, which allows the AI engine to evaluate applicants based strictly on verified qualifications rather than proxy variables (like home addresses or graduation years that can trigger bias), thereby facilitating fairer, more transparent, and legally compliant talent acquisition.

Moreover, as organisations navigate digital transformation, they must develop specialized skills to manage these complex regulatory frameworks (Loidl et al., 2026). Training HR staff to audit AI outputs and understand decentralised architectures is essential to mitigate operational risks and protect candidate rights during automated hiring (Loidl et al., 2026).

E. Identification of Research Gaps

A critical analysis of the current literature reveals several significant gaps. The first is the Immutability vs. Privacy Paradox (GDPR Compliance). While blockchain models (Madhavi & Pande, 2025; Madanchian & Taherdoost, 2026) leverage ledger immutability to prevent fraud, they do not reconcile this with the GDPR 'right to be forgotten' (Article 17). Writing PII directly on-chain or hashing personal data on public registries violates privacy regulations, and the literature lacks a compliant architecture that decouples personal data storage from cryptographic proofs.

The second gap is the Bifurcation between SSI and Machine Learning. Literature is divided into trust-oriented blockchain systems (e.g., Saky et al., 2026) and efficiency-oriented ML screening tools (Amanullah et al., 2026; Zhai et al., 2024). Consequently, unified architectures integrating both are missing. Recruiters must choose between manually verifying credentials or automating screening using unverified, error-prone resume text, perpetuating the 'garbage-in, garbage-out' problem (Cheng & Hackett, 2021).

The third gap is the Scalability and Operational Cost of On-Chain Architectures. Technical prototypes frequently deploy smart contracts directly on public blockchains to execute credential checks (Madhavi & Pande, 2025). This results in high transaction fees and latency, which is unfeasible for enterprise recruiting. The literature lacks frameworks utilizing peer-to-peer protocols (like DIDComm) for off-chain verification, where the blockchain functions purely as a lightweight trust registry.

Finally, the fourth gap is the Lack of Standardized HR Metadata. While W3C standards exist, integration with HR-specific schemas (e.g., HR Open Standards) is missing. Without standardized schemas, automated engines cannot parse credentials without reverting to manual mappings. This research addresses these gaps by proposing a hybrid, four-layer conceptual framework that combines off-chain SSI wallets, W3C specifications, and downstream ML screening in a unified, GDPR-compliant architecture.

3. Research Methodology

A. Research Design

This study employs a conceptual framework and systems architecture design methodology, grounded in the Design Science Research (DSR) paradigm. DSR is particularly suited for addressing complex, multi-stakeholder IT challenges, as it focuses on creating and evaluating innovative artifacts (models, architectures, and frameworks) to solve identified organizational problems. In this research, we translate theoretical cryptographic and decentralisation principles specifically Self-Sovereign Identity (SSI) and public-key infrastructure (PKI) into a functional, multi-layered system model designed for talent acquisition.

Our research design is structured into three iterative phases: requirement identification, architectural design, and protocol formalization. First, we identify key operational and regulatory constraints (e.g., GDPR compliance, CV fraud prevention, and

system scalability) based on our systematic literature synthesis. Second, we design a conceptual four-layer system architecture that modularizes the various components of the recruitment and verification pipeline. Third, we formalize the step-by-step data flows and cryptographic protocols that govern interactions between the primary actors (Issuers, Holders, and Verifiers). Rather than evaluating empirical hiring statistics, this study formalizes the technical specifications, system boundaries, and security relationships necessary to implement a secure, privacy-preserving, and automated credential verification platform. By establishing these architectural foundations, the research bridges the gap between decentralised trust networks and corporate applicant tracking systems (ATS).

B. System Design Requirements & Constraints

To ensure practical viability, regulatory compliance, and security within enterprise recruiting environments, the proposed architecture must satisfy several critical design requirements:

1. *Security & Cryptographic Trust:* The primary security requirement is the absolute tamper-evidence of credentials. Once an educational institution or former employer issues a credential, the data must be cryptographically signed, preventing any unauthorized modification by the applicant or third parties. The verifier must be able to verify the authenticity of the signature and the identity of the signer using the public keys anchored on the blockchain.
2. *Privacy and Regulatory Compliance:* The framework must achieve strict compliance with data protection laws, notably GDPR Article 17 (Right to be Forgotten) and data minimization principles. Personally Identifiable Information (PII) including names, addresses, and transcripts must never be written to the blockchain. All PII must remain in the off-chain data layer, specifically inside the applicant's private digital wallet. Furthermore, the system must support selective disclosure, allowing applicants to generate proofs containing only the requested attributes (e.g., 'Age > 21' or 'Degree = Master of Science') without exposing other sensitive details.
3. *Performance, Scalability, and Cost-Effectiveness:* Enterprise recruitment involves processing thousands of applications. Registering or verifying each candidate on-chain incurs prohibitive transaction fees (gas costs) and suffers from low transaction throughput (Madhavi & Pande, 2025). The system must restrict on-chain writes to one-time operations, such as publishing an Issuer's DID Document or updating cryptographic revocation lists. All credential exchanges, presentations, and verifications must occur off-chain via direct peer-to-peer communication.
4. *Interoperability and Standard Adherence:* To prevent vendor lock-in and enable cross-border verification, the system must adhere strictly to open standards (Budhwar et al., 2022). By implementing W3C Decentralised Identifiers (DIDs) and Verifiable Credentials (VCs), the architecture ensures that credentials issued by diverse global entities can be parsed and verified by any compliant applicant tracking system (ATS).

C. Conceptual Architecture Overview

To satisfy the design requirements, we propose a four-layer conceptual architecture that decouples cryptographic trust from personal data storage.

Layer 1: Verifiable Data Registry (VDR) Layer: As the foundational trust anchor, this public-permissioned blockchain ledger maintains an immutable, globally accessible registry of DIDs, DID Documents (containing public keys and endpoints), credential schemas, and revocation lists. Crucially, no personal data is recorded here, ensuring compliance.

Layer 2: Agent & Protocol Layer: This layer manages encrypted, peer-to-peer communication between actors' agents using the DIDComm protocol. DIDComm secures message routing using asymmetric keys specified in DID Documents. This layer also defines presentation exchange protocols used to request and present credentials.

Layer 3: Data & Wallet Layer: Residing on the candidate's personal device, the SSI wallet stores private keys and Verifiable Credentials issued by academic institutions and employers. The wallet software enables users to approve credential requests, generate proofs, and selectively disclose attributes to recruiters.

Layer 4: Application & Analytics Layer: Deployed in the hiring organization's infrastructure, this layer includes the Verifier Agent, which interfaces with ATS/HRIS and houses the ML screening engine. Once the Verifier Agent confirms presentation validity against the VDR, the validated, structured data is fed directly into the ML engine for ranking.

D. Data Flow and Cryptographic Protocols

The lifecycle of a credential within the proposed framework follows a secure, circular trust flow, governed by cryptographic protocols that eliminate manual verification. The sequence of operations is divided into four distinct phases:

1. *Identity Bootstrap & DID Registration:* Prior to credential exchange, the Issuer and Holder generate key pairs and publish W3C DID Documents containing public keys on the VDR. The Issuer also registers a specific credential schema (defining attributes like 'degreeType', 'major', and 'graduationDate') to standardize the data format.
2. *Credential Issuance:* The Issuer agent generates a Verifiable Credential (VC) containing the candidate's DID as the subject and the academic/employment attributes. Signed with the Issuer's private key, the VC is transmitted securely via DIDComm and stored in the candidate's local wallet.
3. *Presentation Request and Exchange:* When applying for a position, the employer’s Verifier agent sends a presentation request containing a cryptographic challenge (nonce) to prevent replay attacks, alongside

required schema types and specific attributes.

4. *Verification and Ingestion:* Upon user approval, the wallet generates a Verifiable Presentation (VP) signed with the candidate's private key. The VP is sent to the Verifier agent, which resolves the Issuer's DID on the blockchain to retrieve the public key, validates the Issuer's signature, checks revocation status, and verifies wallet ownership via the VP signature. Verified, structured claims are then pushed directly to the ATS and ML pipeline, completing verification in seconds.

4. Analysis & Findings: The Proposed Architecture

The integration of decentralised technologies and machine learning in talent acquisition represents a fundamental shift in how organisations verify credentials, manage data privacy, and automate candidate sifting. To overcome the critical limitations of existing systems—namely, the "Immutability vs. Privacy Paradox" (Madanchian & Taherdoost, 2026), the "garbage in, garbage out" (GIGO) challenge in machine learning screening (Cheng & Hackett, 2021), and the cost and throughput constraints of public blockchain deployments (Madhavi & Pande, 2025)—this paper proposes a decentralised, four-layer system architecture. This architecture separates the core cryptographic trust registry (on-chain) from the transmission and storage of personal credentials (off-chain). It links these verified data points directly with machine learning classification engines for secure, bias-mitigated screening. By doing so, the framework provides an operational mechanism to enforce W3C standards (W3C, 2021, 2022) while fully complying with GDPR (Faruk & Khan, 2022).

A. Layer 1: The Verifiable Data Registry (On-Chain Trust Registry)

The Verifiable Data Registry (VDR) serves as the foundational trust anchor of the proposed architecture. In blockchain-enabled human resource management, early research proposed deploying smart contracts directly on public blockchains (like Ethereum) to register and verify credentials (Madhavi & Pande, 2025). However, storing applicant information directly on-chain exposes companies to high transaction (gas) fees. It violates strict privacy regulations such as the European Union's General Data Protection Regulation (GDPR) Article 17, which mandates the "right to be forgotten." Once data is written to a traditional blockchain, it cannot be deleted or modified, creating a legal and technical deadlock.

The proposed architecture resolves this paradox by using the blockchain strictly as a metadata anchor and trust registry. No PII, candidate names, degrees, or employment histories are ever written to the ledger. Instead, the VDR stores only three types of public cryptographic metadata:

1. *Decentralised Identifier (DID) Documents:* Following the W3C (2022) standard, issuers (such as universities and previous employers) and verifiers (hiring organisations) generate cryptographic key pairs and publish their public keys, cryptographic suites, and service endpoints in a DID Document on the ledger. These DIDs act as verifiable, self-sovereign identities that do not depend on a central authority.
2. *Credential Schemas:* Standardised templates defining the structure of credentials (e.g., fields for a Bachelor of Science degree or a Senior Software Engineer employment history) are published to the VDR. This ensures syntax consistency across different issuers and resolves the metadata fragmentation gap identified by Saky et al. (2026).
3. *Revocation Registry Accumulators:* To handle credential revocation such as when a university rescinds a degree due to academic dishonesty or an employer cancels a professional certificate the VDR maintains cryptographic accumulators (e.g., cryptographic accumulator states or Merkle tree roots). This allows verifiers to check the validity of a credential in real time without learning the identity of the holder or querying the original issuer.

By deploying this registry on a permissioned consortium blockchain (e.g., Hyperledger Indy or a corporate sidechain), the system achieves sub-second latency and near-zero transaction costs, resolving the scalability and cost issues highlighted by Madhavi & Pande (2025) and Madanchian & Taherdoost (2026). The ledger serves only as a trust anchor, validating the signatures of entities involved in credential exchanges while keeping the candidate's actual identity details completely off-chain.

B. Layer 2: The Agent & Protocol Layer (Secure Communication)

The Agent & Protocol Layer governs the secure, peer-to-peer (P2P) communication and cryptographic negotiations between the decentralised participants. In traditional talent acquisition systems, data exchange relies on centralised databases, emails, or APIs, which are highly susceptible to security breaches and lack end-to-end cryptographic trust (Faruk & Khan, 2022). In our architecture, all interactions occur directly between software agents representing the Issuer, Holder (candidate), and Verifier.

The communication is established using the DIDComm Messaging (DIDComm) protocol. DIDComm utilises the public keys and service endpoints defined in the DID Documents on the Verifiable Data Registry to encrypt and route messages. This guarantees that all communication is private, authenticated, and secure against man-in-the-middle attacks.

A key component of this layer is the W3C Presentation Exchange Protocol (2021). When a candidate applies for a role, the hiring organisation's agent sends a presentation request outlining the specific attributes required for the role. For example, rather than demanding the candidate's entire academic transcript (which may contain sensitive demographic data or unrelated grades), the verifier requests only specific proofs, such as a confirmation that the applicant holds a Master's degree in Computer Science from an accredited institution. This design enforces the principle of data minimisation, a core requirement of the GDPR, by allowing the candidate to share only the minimum necessary data to meet the job requirements.

This protocol-level interaction bypasses the need for intermediary third-party screening agencies (Chhetri, 2022), reducing background verification latency from weeks to seconds.

C. The Data & Wallet Layer (Holder-Centric Storage)

The Data & Wallet Layer shifts identity control back to the worker, resolving the centralisation and security risks of traditional corporate databases (Faruk & Khan, 2022). The applicant's credentials are stored in a digital SSI wallet on their local device (e.g., a smartphone or a local desktop app). The wallet holds Verifiable Credentials (VCs) that have been cryptographically signed by authorised issuers (W3C, 2021). These VCs represent academic degrees, previous employment certificates, and professional certifications.

The wallet operates as an encrypted repository. When an applicant receives a presentation request from a verifier, the wallet's cryptographic engine compiles a Verifiable Presentation (VP). To maximise privacy and security, the wallet can generate Zero-Knowledge Proofs (ZKPs). ZKPs allow the applicant to prove the validity of a claim without revealing the underlying data. For instance, an applicant can cryptographically prove they have "more than 5 years of experience in software engineering" or that they graduated before a specific date, without sharing the exact dates, age, or full certificate.

By holding their own data, workers are insulated from the risk of mass corporate data breaches (Faruk & Khan, 2022). If a company is hacked, the attacker cannot steal candidate histories, because the company only verifies cryptographic proofs rather than storing static, unencrypted copies of diplomas and employment letters. This architecture shifts the power dynamics of labour, transferring credential ownership and control back to the individual, aligned with the human-centred agenda described by Cappelli & Rogovsky (2023).

D. Layer 4: The Application & Analytics Layer (ATS & ML Integration)

The Application & Analytics Layer represents the endpoint at which verified, structured data is integrated into the hiring organisation's HR systems, including the Applicant Tracking System (ATS), Human Resource Information System (HRIS), and machine learning (ML) screening engines. A critical vulnerability in modern automated recruiting is the "garbage in, garbage out" (GIGO) problem (Cheng & Hackett, 2021). Traditional ATS systems rely on optical character recognition (OCR) or keyword-based parsing algorithms to extract information from unverified PDF resumes. These resumes are frequently padded, fabricated, or optimized to trick the ATS, resulting in high rates of CV fraud and screening inefficiencies (Saky et al., 2026; Chhetri, 2022).

In the proposed architecture, the verifier agent interfaces directly with the ATS. When a candidate submits their Verifiable Presentation, the system receives structured, machine-readable data formatted in JSON-LD data. This data is cryptographically pre-verified against the blockchain ledger. Consequently, the ATS does not need to parse raw text or perform manual background checks.

The authenticated attributes are directly ingested into an ML classifier. Because the inputs are cryptographically verified, the risk of training or evaluating models on fraudulent data is eliminated, which directly addresses the data quality gaps identified by Amanullah et al. (2026) and Sakib & Islam (2026). Furthermore, the standardised JSON-LD schema (W3C, 2021) enables the extraction of objective, structured inputs (such as specific verified skills, degrees, and employment durations) while omitting subjective or proxy demographic variables (such as candidate photo, name, address, or graduation institution pedigree, if configured). This data minimisation capability helps mitigate algorithmic bias and supports the human-centred agenda advocated by Cheng & Hackett (2021) and Cappelli & Rogovsky (2023). The ML model can focus solely on matching verified skill vectors to job descriptions, thereby increasing screening accuracy and equity.

E. System Walkthrough & Comparative Analysis

1) System Walkthrough: End-to-End Credential Exchange Lifecycle

The operational lifecycle of the proposed architecture consists of five distinct, sequential phases that govern the issuance, storage, verification, and analysis of candidate credentials:

1. *Identity Bootstrapping (DID Creation):* Before any credential exchange can occur, participating entities must establish their digital identities. An educational institution (acting as the Issuer) and a hiring organisation (acting as the Verifier) generate cryptographic key pairs. The author W3C-compliant Decentralised Identifier (DID) Documents containing their public keys, key agreement protocols, and service endpoints (W3C, 2022). These DID Documents are committed to the Verifiable Data Registry (VDR) layer (Layer 1) on the consortium blockchain. Candidates (Holders) also generate their own DIDs, but these remain locally in their SSI wallets, ensuring user-centric sovereignty.
2. *Credential Issuance:* Upon graduation, the educational institution compiles the candidate's degree information (e.g., major, graduation date, institution name) into a structured JSON-LD format complying with W3C Verifiable Credential Data Model guidelines (W3C, 2021). The institution signs this data structure using its private key (associated with its on-chain DID) and transmits the Verifiable Credential (VC) to the candidate's software agent over a secure DIDComm channel. The candidate's SSI wallet (Layer 3) encrypts and stores the VC locally.
3. *Hiring Presentation Exchange Request:* The candidate applies for a vacancy via the hiring organisation's web portal. The organisation's ATS, integrated with a Verifier Agent, initiates a Presentation Exchange protocol. It transmits a request defining the required proof constraints, for instance, "Provide proof of a Bachelor's degree in Computer Science and at least 3

Table 1

Feature/Metric	Centralised HRIS (Masum et al., 2018)	Pure Blockchain Systems (Madhavi & Pande, 2025)	Proposed Decentralised SSI-ML Framework
Data Privacy & GDPR Compliance	High Risk: centralised database stores candidate PII; prone to violations of GDPR Article 17 (Right to be Forgotten).	Non-Compliant: Storing PII or static credential records on an immutable ledger violates the "right to be forgotten" and data minimization.	Fully Compliant: PII is held off-chain in local wallets. The ledger contains only public DIDs, schemas, and revocation states.
Verification Latency	High: Takes weeks due to manual outreach to universities and past employers via third-party screening agencies.	Real-Time On-Chain: Real-time verification of on-chain records, but requires expensive smart contract executions.	Real-Time Off-Chain: Real-time peer-to-peer verification via DIDComm and cryptographic signatures, bypassing gas fees.
Operational & Transaction Cost	Moderate: High operational cost from third-party agency fees ($50–$200 per candidate background check).	High / Volatile: On-chain smart contract execution (gas fees) for every credential validation and update.	Low / Predictable: P2P verification is free. Low consortium ledger anchoring costs for DIDs and schemas.
Data Quality & GIGO Mitigation	Low: High exposure to GIGO (Cheng & Hackett, 2021) due to resume padding, degree falsification, and OCR parsing errors.	High: Data is cryptographically secure on-chain, but lacks automated sifting mechanisms for recruiter ingestion.	Excellent: Complete GIGO elimination. Pre-verified JSON-LD data feeds directly into ML engines, ensuring data integrity and sifting.
Single Point of Failure (SPOF)	Critical: centralised servers represent a high-value target for hackers seeking candidate personal data.	None / Distributed: Ledger is distributed, but candidates' off-chain storage architectures remain unstandardized.	None: Distributed ledger trust registry combined with highly secure, localised, and encrypted holder-centric wallets.

years of software development experience."

4. *Proof Generation & Validation:* The candidate's SSI wallet processes the presentation request, matches it against stored VCs, and prompts the candidate for consent. Upon authorisation, the wallet generates a Verifiable Presentation (VP). For maximum privacy, the wallet can generate a Zero-Knowledge Proof (ZKP) to prove the conditions (e.g., graduation date within a specific range) without revealing the exact certificates. The candidate signs the VP and sends it to the Verifier. The Verifier Agent fetches the Issuer's DID Document from the blockchain, verifies the signature, and checks the cryptographic accumulator state on-chain to ensure the credential has not been revoked.
5. *Analytics Ingestion & Machine Learning Classification:* Once verified, the structured, authenticated attributes (skills, experience, education) are pushed to the Application Layer (Layer 4). The ATS ingests these verified features directly, bypassing the need for manual review or parsing. An ML classification model (e.g., Random Forest or Support Vector Machine) processes this clean dataset, matching candidate qualifications against job requirements without exposure to demographic variables (Cheng & Hackett, 2021), thus ensuring an objective screening process.

F. Comparative Analysis

The table 1 contrasts the proposed Decentralised SSI-ML Framework against conventional centralised Human Resource Information Systems (HRIS) (Masum et al., 2018) and pure on-chain blockchain architectures (Madhavi & Pande, 2025).

5. Conclusion

A. Summary of Contributions

This study addresses the critical security and privacy challenges in digital talent acquisition by proposing a decentralised Self-Sovereign Identity (SSI) framework integrated with machine learning analytics. The main contribution of this research is the conceptualisation and detailing of a four-layer hybrid system architecture that successfully resolves the "Immutability vs Privacy Paradox" (Madanchian & Taherdoost, 2026; Faruk & Khan, 2022). By leveraging W3C standard Decentralised Identifiers (DIDs) and Verifiable Credentials (VCs) (W3C, 2021, 2022) with off-chain storage, the architecture satisfies the stringent requirements of GDPR Article 17 (Right to be Forgotten) while maintaining the tamper-proof cryptographic trust of blockchain technology. Furthermore, this framework bridges the gap between decentralised identity systems and automated recruitment technologies. It introduces a mechanism that enables machine learning models to ingest pre-verified, structured JSON-LD credential data directly from applicant wallets. This integration eliminates the "garbage in, garbage out" (GIGO) limitation identified in traditional Applicant Tracking Systems (ATS) and ML screening systems (Cheng & Hackett, 2021; Saky et al., 2026), replacing unverified, text-based resumes with cryptographic evidence of qualification.

B. Theoretical Implications

The theoretical value of this framework lies in its convergence of two previously distinct fields: distributed systems (blockchain and SSI) and algorithmic human resource management (ML screening). In the domain of Strategic Human Resource Management (SHRM), this architecture modifies the power dynamics of labour. As critiqued by Cappelli & Rogovsky (2023) and Cheng & Hackett (2021), corporate-centric HR practices often treat candidate data as organisational property, forcing applicants to surrender personal information to centralised corporate silos. By shifting control to a holder-centric wallet layer, this architecture operationalises the principles of worker agency and data sovereignty. It establishes that credential ownership belongs to the worker, not the institution. Furthermore, the study contributes to AI ethics literature (Agwu, 2026; Patnaik, 2026) by demonstrating how cryptographic data minimisation and Zero-Knowledge Proofs (ZKPs) can be used to mitigate algorithmic bias. Rather than adjusting ML models after training to reduce bias, this framework prevents bias at the ingestion level by removing proxy demographic variables and

feeding only verified, relevant skill vectors into the classifier.

C. Practical & Managerial Implications

From a managerial perspective, implementing this decentralised SSI-ML framework offers significant operational advantages. First, it reduces background screening times from weeks to seconds. By eliminating third-party background check agencies (Madhavi & Pande, 2025; Chhetri, 2022), organisations can drastically decrease time-to-hire and administrative costs. Second, the complete elimination of resume fraud at the intake level safeguards organisations from negligent hiring liabilities, financial losses, and reputational damage. Recruiters no longer need to verify candidate claims manually, as the data is cryptographically verified in advance. Finally, the framework enhances the cybersecurity profile of hiring organisations. By verifying cryptographic proofs instead of storing unencrypted candidate credentials (such as passport copies, academic transcript PDFs, and past contracts), organisations reduce their exposure to data breaches and minimise compliance risks under global data protection laws (Faruk & Khan, 2022). This allows HR departments to transition from clerical record-keeping units to strategic, secure, and privacy-compliant decision centres.

6. 7. Suggestions/Recommendations

A. Technical Recommendations for HR Tech Developers

To successfully implement the proposed architecture, HR technology developers and software engineers should focus on interoperability and open standards. We recommend that developers avoid proprietary identity systems and instead build their systems using the W3C Decentralised Identifiers (DIDs) standard (W3C, 2022), the W3C Verifiable Credentials Data Model (W3C, 2021), and the open protocols defined by the Decentralised Identity Foundation (DIF). This ensures that corporate platforms can verify credentials issued by any standard-compliant university or employer globally, preventing vendor lock-in.

Furthermore, developers should build modular, API-driven integration plugins for existing Applicant Tracking Systems (ATS) and Human Resource Information Systems (HRIS), such as the iHRIS model proposed by Masum et al. (2018). These plugins should act as middleware that translates incoming JSON-LD verifiable presentations into structured feature vectors for machine learning pipelines. Finally, developers must prioritise implementing zero-knowledge proof (ZKP) cryptographic libraries (such as BBS+ signatures or CL-signatures) in mobile wallet applications to enable privacy-preserving credential presentations.

B. Policy and Regulatory Recommendations

The successful deployment of decentralised credentialing systems requires cooperation across multiple sectors. We recommend establishing global credential verification consortia comprising academic institutions, corporate federations, professional licensing bodies, and government identity registries. These consortia should define standardised credential schemas (e.g., HR Open Standards/HR-XML) for common qualifications, job titles, and skill sets, ensuring semantic interoperability across industries.

Additionally, policymakers and data protection authorities (such as the European Data Protection Board) should issue clear regulatory guidelines endorsing the use of SSI frameworks as a compliant method for digital background checks. Regulators should establish sandbox environments where organisations can test blockchain-based identity registries without facing compliance penalties. Finally, academic institutions should be incentivised to digitise their degree issuance processes by integrating VC-signing keys directly into their registrar systems, thereby creating a reliable network of trusted issuers.

C. Future Research Scope

While this study provides a conceptual framework and system architecture, future research should focus on empirical testing and validation. Researchers should build functional prototypes of the proposed architecture and conduct load testing under simulated enterprise volumes to evaluate the throughput, latency, and performance of off-chain DIDComm agents. Additionally, empirical studies should analyse the gas efficiency of consortium blockchain ledgers when anchoring high volumes of DID registrations and credential revocation states.

Another promising direction for future research is the integration of decentralised confidential computing techniques, such as Multi-Party Computation (MPC) or Homomorphic Encryption. These technologies could enable machine learning models to rank candidates based on verified credentials while keeping those credentials fully encrypted, ensuring candidate data is never exposed during the screening process. Finally, future studies should conduct qualitative user research to explore candidate and HR professional perceptions of usability, trust, and acceptance of SSI technologies in talent acquisition, extending the Technology Acceptance Model (TAM) analysis discussed by Obizue (2026).

References

[1] N. Abadi and S. Outmane, "Systematic Review and Bibliometric Analysis of Artificial Intelligence Adoption in Human Resource Management," *Sustainability*, vol. 18, no. 2, pp. 112–135, 2026.

[2] D. J. Agwu, "Artificial intelligence and human resource management: HR analytics, talent management, and ethical AI," *Int. J. Appl. Resilience Sustainability*, vol. 2, no. 2, pp. 989–1013, 2026.

[3] M. Amanullah, M. F. Ahmed, K. K. Tumpa, M. Khatun, R. K. Paul, and P. Tarafdar, "Artificial intelligence for data-driven human resource decision-making: A systematic review," *Social Sci. Humanities Open*, vol. 13, Art. no. 102909, 2026.

[4] S. Batra and R. Sharma, "Blockchain-Enabled Business Intelligence for Human Resource Information Systems and Payroll Platforms," *Amer. J. Scholarly Res. Innov.*, vol. 1, no. 2, pp. 30–58, 2022.

[5] S. Bondarenko and R. Mylyanyk, "Digital Transformation of Human Resource Policies: Integrating AI and Data Analytics in Strategic Workforce Management," *Social Dev.: Econ. Legal Issues*, vol. 10, pp. 695–715, 2025.

[6] P. Budhwar, A. Malik, M. T. T. De Silva, and P. Thevisuthan, "Artificial intelligence – challenges and opportunities for international HRM: a review and research agenda," *Int. J. Hum. Resour. Manage.*, vol. 33, no. 6, pp. 1065–1097, 2022.

[7] P. Cappelli and N. G. Rogovsky, "Artificial intelligence in human resource management: A challenge for the human-centred agenda?" ILO Working Paper, No. 95, International Labour Organisation, Geneva, Switzerland, 2023.

[8] A. M. Căvescu and N. Popescu, "Predictive Analytics in Human Resources Management: Evaluating AIHR's Role in Talent Retention," *Appl. Math.*, vol. 5, no. 2, pp. 558–574, 2025.
[9] M. M. Cheng and R. D. Hackett, "A critical review of algorithms in HRM: Definition, theory, and practice," *Hum. Resour. Manage. Rev.*, vol. 31, no. 1, Art. no. 100752, 2021.
[10] H. Chalutz Ben-Gal, "An ROI-based review of HR analytics: practical implementation tools," *Personnel Rev.*, vol. 48, no. 6, pp. 1429–1448, 2019.
[11] R. Chhetri, "Implementation of Blockchain Technology in Human Resource Recruitment," Bachelor's thesis, School of Business, Jamk Univ. of Appl. Sci., Jyväskylä, Finland, 2022.
[12] O. M. Faruk and M. K. Khan, "Blockchain-enabled BI for HR and payroll systems: Securing sensitive workforce data," *Amer. J. Scholarly Res. Innov.*, vol. 1, no. 2, pp. 30–58, 2022.
[13] A. L. Jimoh, "Talent management and employee performance in the age of artificial intelligence: A systematic literature review," *Edelweiss Appl. Sci. Technol.*, vol. 10, no. 7, pp. 22–36, 2026.
[14] S. Jooss, A. McDonnell, and R. Burbach, "Talent designation in practice: an equation of high potential, performance and mobility," *Int. J. Hum. Resour. Manage.*, vol. 30, no. 2, pp. 744–762, 2019.
[15] G. Koştı and İ. Kayadibi, "A bibliometric analysis of artificial intelligence and machine learning applications for human resource management," *Future Bus. J.*, vol. 11, no. 1, pp. 179–195, 2025.
[16] J. Kovac *et al.*, "Systematic Review and Bibliometric Analysis of Artificial Intelligence Adoption in Human Resource Management," *Sustainability*, vol. 17, no. 4, pp. 450–475, 2025.
[17] C. Kumar and A. Kumar, "Design and Implementation of a Blockchain-Based Person Verification System for HR Operations," *J. Eng. Technol. Manage.*, vol. 76, pp. 1640–1662, 2025.
[18] V. Loidl, N. Zulauf, J. S. Sung, and M. Chahine, "Preparing organisations for Digital Transformation: A Systematic Literature Review of Skill Development," *Int. J. HRD: Pract. Policy Res.*, vol. 10, no. 1, pp. 86–102, 2026.
[19] M. Madanchian and H. Taherdoost, "Blockchain-Enabled Human Resource Management for Enhancing Transparency, Trust, and Talent Mobility in the Digital Era," *Blockchains*, vol. 4, no. 1, pp. 1–22, 2026.
[20] C. B. Madhavi and A. Pande, "Design and Implementation of a Blockchain-Based Person Verification System for HR Operations," *J. Eng. Technol. Manage.*, vol. 76, pp. 1640–1662, 2025.
[21] A. K. Masum, L. S. Beh, A. K. Azad, and K. Hoque, "Intelligent Human Resource Information System (iHRIS): A Holistic Decision Support Framework for HR Excellence," *Int. Arab J. Inf. Technol.*, vol. 15, no. 1, pp. 121–130, 2018.
[22] M. N. Obizue, "Acceptance of artificial intelligence in human resource management: Adoption factors, technology acceptance models, and HR analytics," *Int. J. Appl. Resilience Sustainability*, vol. 2, no. 2, pp. 1037–1066, 2026.
[23] A. Patnaik, "Artificial intelligence in human resource management: A review of applications, algorithms, and ethical challenges," *Int. J. Appl. Resilience Sustainability*, vol. 2, no. 2, pp. 869–895, 2026.
[24] T. Peeters, J. Paauwe, and K. Van De Voorde, "People analytics effectiveness: developing a framework," *J. Organ. Effectiveness: People Perform.*, vol. 7, no. 2, pp. 203–219, 2020.
[25] K. Y. Ping and R. Sakaki, "Strategic human resource management in the future of work: A systematic review of digital transformation, inclusion, and sustainability," *J. Bus. Manage. Accounting*, vol. 16, no. 1, pp. 57–81, 2026.
[26] M. N. Sakib and S. Islam, "The impacts of machine learning on human resource management: a systematic literature review and bibliometric analysis," *Future Bus. J.*, vol. 12, no. 1, pp. 7–23, 2026.
[27] S. M. A. I. Saky, F. Akter, R. Islam, Y. Akter, and J. Islam, "Blockchain and Machine Learning in Talent Acquisition: A Review on Credential Verification and Recruitment Optimisation," *Informatica Economică*, vol. 30, no. 1, pp. 54–68, 2026.
[28] M. A. Suárez Pizzarello, E. A. Rodríguez Flores, L. F. Garcés Giraldo, A. Valencia-Arias, J. C. Patiño-Vanegas, S. Cardona-Acevedo, and M. L. Benjumea-Arias, "Artificial Intelligence in Human Resources: A Systematic Review," *Int. J. Aquatic Res. Environ. Stud.*, vol. 6, no. S1, pp. 1–14, 2026.
[29] D. Vrontis, M. Christofi, V. Pereira, S. Tarba, A. Makrides, and E. Trichina, "Artificial intelligence, robotics, advanced technologies and human resource management: a systematic review," *Int. J. Hum. Resour. Manage.*, vol. 32, no. 1, pp. 1–30, 2021.
[30] Y. Zhai, L. Zhang, and M. Yu, "AI in Human Resource Management: Literature Review and Research Implications," *J. Knowl. Econ.*, vol. 15, no. 1, pp. 1–25, 2024.
[31] W3C, "Decentralised Identifiers (DIDs) v1.0: Core Data Model, Schema, and Representations," W3C Recommendation, World Wide Web Consortium, 2022.
[32] W3C, "Verifiable Credentials Data Model v1.1," W3C Recommendation, World Wide Web Consortium, 2021.