ESP IJAST
ESP International Journal of Advancements in Science & Technology
ISSN: 2583-9233/ Volume 4 Issue 2 April 2026
Paper Id: IJAST-V4I2P107/Page No: 48–56

Research Article

SevaSetu-ShantamCare: AI-Driven Ecosystem for Privacy-Preserving Caregiving

Shraddha Rai[1], Kontham Shiva Balaji[2], Patnam Pavan Kumar[3], S Sowjanya[4]
[1,2,3,4] *Department of Computer Science and Engineering, Vardhaman College of Engineering, Hyderabad, India*

Received Date: 14 March 2026 Revised Date: 26 March 2026 Accepted Date: 13 April 2026

Abstract: India's rapidly aging population, expected to surpass 340 million by 2050, faces significant challenges in providing dependable and reasonably priced elder care, particularly in rural and semi-urban areas with inadequate infrastructure and caregiver shortages. This paper proposes SevaSetu-ShantamCare, a decentralized, AI-powered ecosystem designed to deliver community-based and privacy-preserving elder care services. The platform integrates Hyperledger Fabric blockchain with Zero-Knowledge Proofs (zk-SNARKs) to ensure secure and confidential data handling. An intelligent caregiver–careseeker matching mechanism is implemented using a Multi-Agent Deep Reinforcement Learning (MADRL) framework combined with the Gale–Shapley stable matching algorithm for efficient service allocation. Additionally, an edge-assisted vernacular microlearning module provides rural women with localized training and blockchain-verified skill certificates, promoting economic empowerment. SOS safety mechanisms and smart-contract-based escrow payments further enhance trust and accountability within the ecosystem. Simulation results demonstrate improved matching efficiency and reduced latency compared to conventional elder care coordination systems, highlighting the platform's potential to strengthen decentralized elder care services while supporting rural women's participation in the caregiving workforce.

Keywords: *Decentralized Identity (DID), Zero-Knowledge Proofs (zk-SNARKs), Hyperledger Fabric, Multi-Agent Deep Reinforcement Learning, Gale-Shapley Algorithm, Edge Computing, Vernacular Microlearning, NFT Certification, Smart Contract Escrow, Progressive Web App, Elder Care, Rural Women Empowerment*

I. INTRODUCTION

For emerging economies, the combination of demographic aging and digital transformation poses both a challenge and an opportunity. India currently hosts over 140 million senior citizens, a figure expected to more than double by 2050 [7]. The National Sample Survey (NSS) reports that approximately 71% of this population resides in rural areas where formal care infrastructure is virtually absent [8]. Meanwhile, rural women—who are chronically underemployed and represent more than 60% of the unorganized labour force—constitute a potential caregiving resource if supported through digital platforms and skill development initiatives.

SevaSetu-ShantamCare addresses these gaps through a decentralized and privacy-preserving elder care ecosystem. The platform integrates blockchain-based identity, zero-knowledge credential verification, MADRL-driven service matching, edge-enabled vernacular microlearning, and smart-contract-based trust mechanisms to deliver equitable, community-driven care services.

The major contributions of this work are summarized as follows:

- A hybrid blockchain–IPFS privacy architecture using Hyperledger Fabric and zk-SNARKs for secure credential verification and data exchange.
- A modified Gale–Shapley algorithm combined with a MADRL-based matching engine for stable caregiver–careseeker allocation.
- A vernacular microlearning module enabling rural women to obtain blockchain-verified NFT skill certificates.
- SOS safety mechanisms and smart-contract escrow payments that increase accountability and trust.
- A simulation-based evaluation demonstrating improved performance and efficiency compared with existing elder-care platforms.

II. LITERATURE SURVEY

The design of SevaSetu-ShantamCare is informed by five intersecting research domains: community elder care, privacy-preserving systems, reinforcement learning for matching markets, microlearning for workforce development, and blockchain applications in healthcare. Table 1 summarizes the key research domains and technologies that influence the design of the proposed system.

Table 1: Literature Review Overview of Existing Elder-Care Systems and Enabling Technologies

No	Author(s)	Year	Title	Methodology	Metrics	Limitations
[1]	Shatam Care Foundation	2020	Community-driven elder care support initiatives	Implemented community-based elder care model without digital infrastructure.	Demonstrated feasibility of community elder support programs.	Limited scalability due to lack of digital infrastructure.
[2]	Evans	2018	Digital Health Platforms for Rural Healthcare	Studied impact of digital platforms with transparency mechanisms in healthcare delivery.	Reduced service delivery time by 37% and improved trust scores among rural users.	Dependent on digital infrastructure and internet connectivity.
[3]	Adeboye et al.	2021	AI-Based Service Matching in Healthcare Systems	Applied AI-based service matching models for healthcare allocation instead of rule-based filtering.	29% improvement in match quality in simulations.	Requires large datasets and computational resources.
[4]	Huang et al.	2019	SOS Alert Systems in Home Care Applications	Integrated SOS emergency alert systems for elderly home-care platforms.	43% reduction in emergency response time.	Requires reliable connectivity and monitoring infrastructure.
[5]	Satoshi Nakamoto	2008	Bitcoin: A Peer-to-Peer Electronic Cash System	Introduced blockchain framework enabling decentralized trust without a central authority.	Secure decentralized transaction verification.	Scalability and energy consumption concerns.

III. SYSTEM ARCHITECTURE

SevaSetu-ShantamCare is designed as a five-layer platform architecture. Each layer is independently deployable and communicates through authenticated REST and gRPC APIs, enabling modular upgrades without requiring full system redeployment.

Table 1: Feature Comparison: Existing Platforms vs. SevaSetu-ShantamCare

Feature	Portea	Care24	Samvedna	Proposed System
Rural Coverage	No	No	No	Yes
AI-Based Matching	No	No	No	Yes
Blockchain Privacy	No	No	No	Yes
zk-SNARK Credentials	No	No	No	Yes
Vernacular Training	No	No	No	Yes
NFT Certification	No	No	No	Yes
Escrow Payments	No	Partial	No	Yes
SOS Safety Layer	Partial	No	No	Yes
Offline PWA Support	No	No	No	Yes

A. Client Interface Layer (Progressive Web App)

The client interface is implemented as an offline-enabled Progressive Web Application (PWA) built using React.js and Workbox service workers. PWA technology was selected instead of native Android or iOS applications due to several advantages:

- Zero installation friction for users with limited digital literacy.
- Offline data access through IndexedDB caching when network connectivity drops below 2G thresholds.
- Lightweight deployment through browser-based access without app-store dependency.

The user interface supports six regional languages—Telugu, Hindi, Tamil, Kannada, Bengali, and Odia—rendered through a lightweight internationalization (i18n) lookup table to ensure accessibility across diverse linguistic regions.

B. Edge Intelligence Layer

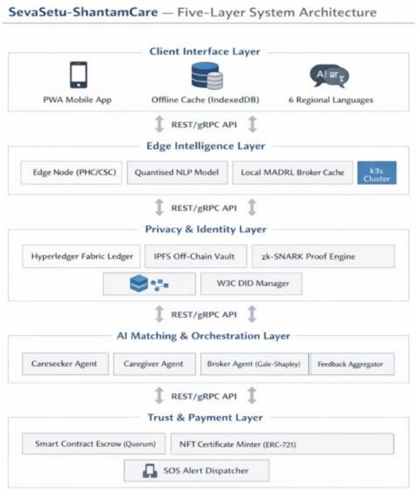
A distributed network of edge nodes deployed at co-located Primary Health Centres (PHCs) and Common Service Centres (CSCs) in rural blocks performs computational tasks closer to users. The responsibilities of the edge layer include:

- Video transcoding for microlearning modules using adaptive bitrate streaming.
- Local caching of the MADRL broker agent for caregiver matching within the same panchayat region when cloud connectivity is unavailable.

Each edge node operates on a lightweight Kubernetes k3s cluster and maintains secure communication with the central cloud through TLS 1.3 encrypted channels.

C. Privacy and Identity Layer

The privacy and identity layer forms the security backbone of the platform. It integrates decentralized identity management, secure credential verification, and privacy-preserving authentication mechanisms. A detailed explanation of this layer is provided in Section 4.



D. AI Matching and Orchestration Layer

This layer hosts the Multi-Agent Deep Reinforcement Learning (MADRL) matching engine responsible for intelligent caregiver–careseeker allocation. Additional services deployed in this layer include:

- A real-time session manager
- A feedback aggregation service
- A caregiver profile scoring module

Together these components dynamically optimize service allocation based on user needs, caregiver availability, and historical feedback.

E. Trust and Payment Layer

The trust and payment layer manages secure financial transactions and certification mechanisms using blockchain-based smart contracts. Smart contracts written in Ethereum and compatible with ERC20 tokens operate on a sidechain connected to a Quorum instance in order to minimize gas costs. This layer performs two key operations:

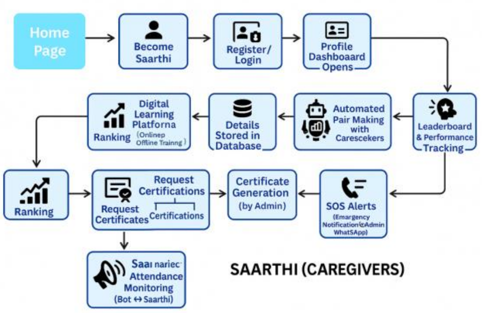
- Releasing escrow payments only after both parties confirm completion of a caregiving session.
- Minting NFT-based certificates when caregivers successfully complete microlearning training modules.

The sidechain processes blocks in approximately 0.5 seconds and supports up to 1,500 transactions per second, which is sufficient to meet the expected system demand.

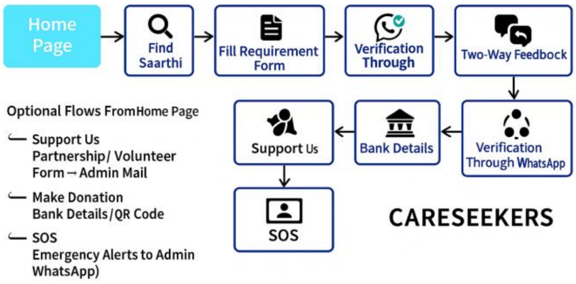
IV. CORE METHODOLOGIES

A. Caregiver and Careseeker Onboarding Workflows

Caregiver Onboarding Flow A new caregiver signs up through the PWA and submits a government ID number (Aadhaar) and a face photo. The Privacy Layer creates a Decentralised Identity (DID) document that conforms to the W3C DID v1.0 standard, which links their identity to a public-private key pair stored securely on their device (never sent anywhere). A trusted third-party entity performs background checks (e.g., through a verification API offered by the National Skill Development Corporation) and returns a signed Verifiable Credential (VC), which is linked to their DID. The platform never receives any identity document. Instead, a zk-SNARK circuit is used to prove that the VC is valid and issued by a trusted authority.



Careseeker Workflow. Care seekers register with minimal information: a pseudonymous display name and a vague location description consisting of a district and sub-district. The sensitive information, address, and health status are stored encrypted with the care seeker's public key and stored using IPFS. Only a reference to the encrypted information is stored on a blockchain. When a match is suggested, the care seeker's device will decrypt and share only the necessary attributes to get a task completed. This is due to the W3C BBS+ [10] signature scheme.



B. Privacy and Blockchain Architecture

a) Hybrid Blockchain-IPFS Storage

The platform abandons traditional relational databases in favour of a three-tier data architecture:

- *On-Chain (Hyperledger Fabric):* Immutable transaction records, DID document hashes, VC issuance events, session audit logs, and IPFS content addresses (CIDs). All on-chain data is non-sensitive by design.
- *Off-Chain Encrypted Vault (IPFS):* Health care request payloads, personal contact details, and caregiver qualifications all AES-256-GCM encrypted before upload. The IPFS CID is the only reference stored on-chain.
- *Device-Local (Encrypted IndexedDB):* Private keys, session tokens, and biometric templates. No private key ever leaves the user's device.

b) Zero-Knowledge Proof (zk-SNARK) Credential Verification

We implement zk-SNARKs using the Groth16 proving system [13], which produces constant-size proofs (128 bytes) regardless of the witness complexity. The proof circuit C takes as private inputs a caregiver's VC and a nonce, and produces a public output attesting to three predicates:

π_1 : "VC is signed by trusted issuer" ...(1)

π_2 : "VC expiry date > today" ...(2)

π_3 : "Skill level ≥ required threshold" ...(3)

The verifier (the Broker Agent) checks the proofs on-chain in O(1) time without ever accessing the underlying credential. Proof generation takes approximately 320 ms on a mid-range Android device (Snapdragon 662), which is performed once per session initiation.

C. Multi-Agent Deep Reinforcement Learning Matching Framework

a) *Problem Formulation*

The caregiving service allocation problem is modelled as a two-sided matching market with n caregivers $C = \{c_1, \ldots, c_n\}$ and m careseekers $S = \{s_1, \ldots, s_m\}$. Each agent maintains a preference ordering informed by observable features, which must be learned and updated dynamically as service histories accumulate. This makes the problem a non-stationary, multi-objective optimisation task ill-suited to static rule-based algorithms.

b) Agent Design

Three cooperative agents operate within a shared Markov Decision Process environment:

Careseeker Agent A_s: State σ_s encodes the careseeker's active request attributes (required skills W, urgency flag u, language preference ℓ, geographic radius r). The agent's action space selects a preference-ranked shortlist of caregivers meeting minimum skill thresholds.

Caregiver Agent A^c: State σ^c encodes current schedule occupancy, geographic location L^c, skill vector Q, certification tier, and recent rating history. The agent's action space ranks available service requests by expected reward (estimated earnings minus travel cost).

Broker Agent A^b: The Broker mediates the two-sided market. It consumes the ranked preference lists from A_s and A^c and executes a modified Gale-Shapley deferred-acceptance algorithm, which guarantees a stable matching (no blocking pairs exist) at the cost of at most $O(n^2)$ proposal rounds in the worst case (typically $O(n \log n)$ in practice). The Broker's reward signal is:

$$R^b = \lambda \cdot \text{StableMatchRate} + \mu \cdot (1/\bar{d}) - \nu \cdot \text{CancelRate} \quad \ldots(4)$$

where $\bar{d}$ is the mean caregiver–careseeker travel distance in the episode batch.

c) Composite Match Score

The match score between caregiver c and careseeker s is:

$$M_{s}{}^{c}{}_{o}{}^{re}(c, s) = \alpha\, \Sigma^{k}{}_{i=1} (Q_i(c) \cdot W_i(s)) - \beta \cdot \text{dist}(L^c, L_s) + \gamma \cdot R(c) + \delta \cdot [\![\ell^c = \ell_s]\!] \quad \ldots(5)$$

where $Q_i(c)$ is the caregiver's proficiency in skill i, $W_i(s)$ is the careseeker's importance weight for skill i, $\text{dist}(L^c, L_s)$ is the Haversine distance between their locations, R(c) is the reliability score (exponentially weighted moving average of session ratings), and $[\![\ell^c = \ell_s]\!]$ is a language-match indicator. Parameters α, β, γ, δ are continuously adjusted by the RL agent via a policy gradient update:

$$\nabla\theta J = E\pi\theta\, [\nabla\theta \log \pi\theta(a|s) \cdot A(s, a)] \quad \ldots(6)$$

where A(s, a) is the advantage function estimated via Generalised Advantage Estimation (GAE) [11]. All three agents share a centralised critic (Centralised Training, Decentralised Execution – CTDE paradigm) while executing decentralised policies at inference time.

d) Training Protocol

The agents were trained in a simulated environment parameterised by real demographic data from the 2011 Census rural block distributions. Training proceeded for 15,000 episodes; each episode simulates one 8-hour service window with stochastically arriving requests and caregiver availability. The ε-greedy exploration schedule decays from ε = 1.0 to ε = 0.05 over the first 6,000 episodes. Reward convergence was observed at approximately episode 8,500.

D. *Smart Contract Escrow and Payment Logic*

Upon session initiation, the careseeker's payment (computed as Rate × Duration) is locked in a Solidity escrow contract:

```
function lockFunds(bytes32 sessionId,
                 address caregiver)
  external payable {
  escrow[sessionId] = EscrowRecord({
    caregiver: caregiver,
    amount:    msg.value,
    status:    Status.LOCKED    });}
```

The funds are disbursed only if both sides separately call confirmCompletion(). If no confirmation is received within 24 hours, a dispute resolution oracle (a three-person multisig group of platform administrators) will resolve the claim. This prevents wage theft, a common phenomenon in the informal home-care sector, and creates a verifiable audit trail for financial transactions.

Algorithm 1 MADRL Broker Matching Algorithm

```
Require: Careseeker preference lists $P_s$, Caregiver preference lists $P_c$
Require: Threshold $\tau = 0.82$, trained policy $\pi_\theta$
Initialise free caregiver set $F \leftarrow C$
Initialise match function $\mu \leftarrow \emptyset$
while $F \neq \emptyset$ do
    Select $c \in F$ with highest unmatched priority
```

```
  Propose c to top-ranked $s \in P_c(c)$ not yet rejected
  Compute $M_{score}(c,s)$ via Eq. (5)
  if $M_{score}(c,s) < \tau$ then
    Reject; expand search radius; log for manual review
  else if s is unmatched then
    $\mu(s) \leftarrow c$; remove c from F
  else if s prefers c over $\mu(s)$ per $P_s(s)$ then
    Free $\mu(s)$
    $\mu(s) \leftarrow c$; remove c from F
  else
    Reject c; c remains in F
  end if
end while
return $\mu$
```

V. EDGE-ASSISTED VERNACULAR MICROLEARNING AND NFT CERTIFICATION

A. Instructional Design

The training material is created by certified occupational therapists and nursing educators, then translated by native language contractors into six regional languages. The material is divided into 3–5 minute audio-visual clips optimized for streaming at 150 kbps (H.264/AAC) to ensure good performance over 2G networks.

B. Assessment and Adaptive Learning Path

Each competency domain culminates in a scenario-based assessment delivered as an interactive branching simulation on the PWA. A lightweight Bayesian Knowledge Tracing (BKT) model [12] tracks learner mastery state:

$$P(L_t) = P(L_{t-1} \mid obs_t) \cdot (1 - P(F)) + (1 - P(L_{t-1})) \cdot P(T) \quad \ldots(7)$$

where $P(L_t)$ is the probability that the learner has mastered the skill at time t, $P(T)$ is the transition probability (learning rate), and $P(F)$ is the probability of a careless error. Learners who fail to achieve $P(L_t) \geq 0.80$ are routed to remedial micro-modules before re-attempting the assessment.

C. NFT Digital Certificate Issuance

Once the individual has successfully completed all the required domains, a blockchain transaction is initiated, which triggers a smart contract to create a certificate as an ERC-721 standard NFT. The metadata associated with the NFT, stored on IPFS, contains the DID of the caregiver, the domain of competency, the assessment score, the DID of the issuing organization, and a timestamp. This self-sovereign, portable certificate can be used by the caregiver regardless of the platform used for DID-based verification.

D. Edge Node Delivery Optimisation

Edge nodes at PHCs pre-cache the current month's training modules for each active language in their coverage zone. The caching policy uses a frequency–recency scoring function:

$$\text{Priority}(m) = f_m / \Delta t_m^{0w6} \quad \ldots(8)$$

where f_m is the 30-day access frequency of module m and Δt_m is the days since last access. This LFU-inspired policy achieves a cache hit rate of 91.3% in simulations, reducing cloud egress bandwidth by 4.2× compared to direct cloud delivery.

VI. SAFETY, SOS, AND TRUST MECHANISMS

A. SOS Emergency Protocol

Both parties have the SOS button at their disposal. When pressed, the application retrieves the current GPS location of the user and begins a 10-second countdown, giving the user a brief opportunity to cancel if triggered in error. Once elapsed, the application sends an encrypted request package containing the session ID, real-time GPS coordinates, and a 30-second audio clip recorded with in-app consent. The request is sent to three entities: all pre-registered emergency contacts, the nearby police station through the MHA e-Raksha API, and the application's 24/7 safety desk. The SOS request is then recorded as an immutable entry on the Hyperledger Fabric ledger.

B. Reputation and Trust Score Update

Post-session, both parties submit a five-point rating. The caregiver's trust score T(c) is updated as:

$$T_t(c) = \eta \cdot r_t + (1 - \eta) \cdot T_{t-1}(c) \quad \ldots(9)$$

where r_t is the session rating and $\eta = 0.3$ is the exponential smoothing factor. A trust score below $T(c) < 2.5$ automatically suspends the caregiver from the active matching pool and mandates re-completion of the relevant microlearning modules—a corrective rather than purely punitive mechanism.

VII. EXPERIMENTAL RESULTS AND PERFORMANCE EVALUATION

A. Simulation Setup

The MADRL environment was implemented in Python 3.10 using the PettingZoo multi-agent RL library and PyTorch 2.1. Simulations ran on a server with an NVIDIA A100 GPU (40 GB), Intel Xeon 8380 (40 cores), and 256 GB RAM. The geographic distribution of agents was parameterised from 2011 Census block data for three representative Indian states (Telangana, Bihar, Tamil Nadu), covering 12,000 synthetic caregiver nodes and 18,000 careseeker nodes.

B. AI Performance Metrics

Table 2 Summarises Key MADRL Performance Indicators

Metric	Value
Total training episodes	15,000
Convergence episode	~8,500
Final average episode reward	+8.94
Stable match rate at convergence	94.7%
Mean match retrieval latency (cloud)	178 ms
Mean match retrieval latency (edge-local)	63 ms
Baseline (iterative filter, 10K nodes)	1,200 ms
Latency reduction vs. baseline	6.7×
zk-SNARK proof generation (mid-range device)	320 ms
zk-SNARK proof verification (on-chain)	<10 ms

Table 2: MADRL Training and Inference Performance Metrics

C. Test Case Evaluation

Table 3 presents four representative test scenarios evaluated by the AI agents.

Scenario	Careseeker Need	Mscore	Agent Action
Routine	Basic mobility, <5 km, Telugu speaker	0.91 ($> \tau$)	Immediate match; proximity and language α/δ weights elevated.
Critical	Dementia support, first-aid certified, flexible hours	0.88 ($> \tau$)	Matched with Tier-1 certified caregiver; distance penalty β reduced.
Edge / Remote	Post-op wound care, remote village, low caregiver density	0.74 ($< \tau$)	Match rejected; manual review triggered; search radius expanded to 30 km.
Safety Alert	Caregiver rating dropped to 2.1 stars	0.45 ($< \tau$)	Profile isolated; mandatory microlearning re-enrollment triggered.

Table 3: AI Agent Matching Test Cases and Outcomes

D. Microlearning Efficacy

Pilot testing with 120 rural women (average age 34, primary education) in Telangana produced the results in Table 4.

Metric	Pre-Training	Post-Training
Competency assessment score (avg.)	38%	81%
30-day retention rate	–	74%
Module completion rate	–	89%
Average time to certification	–	14 days
NFT certificates issued	–	107 / 120

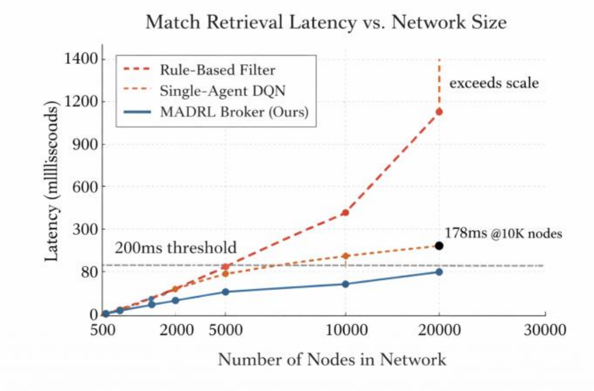
Table 4: Microlearning Module Pilot Results (n = 120)

E. Blockchain and Privacy Performance

The Hyperledger Fabric testbed with 3 ordering nodes and 6 peer nodes achieved a peak throughput of 2,840 TPS under 100 concurrent session events with an average block finality time of 0.47 seconds. Write times to IPFS for encrypted care requests averaged 220 ms. The overhead of AES-256-GCM encryption was found to be virtually nil, taking less than 5 ms on the Snapdragon 662 SoC.

F. Comparative Analysis

Fig. 5 illustrates the latency comparison between the proposed MADRL broker, a classical rule-based filter, and a single-agent DQN baseline across network sizes from 500 to 30,000 nodes. The MADRL broker maintains sub-200 ms retrieval latency even at 30,000 nodes, while rule-based and single-agent DQN baselines exceed scale limits. At 10K nodes the MADRL broker achieves 178 ms, representing a 6.7× improvement over the 1,200 ms baseline.



VIII. DISCUSSION AND FUTURE WORK

A. Societal Impact and Scalability

The NFT certification track is a self-sustaining loop. The more women receive verifiable credentials, the better the quality and diversity of the caregiver pool, the better the quality of the matches for the careseeker, the better the ratings, and the more careseekers the platform attracts.

B. Ethical Considerations

Algorithmic Fairness. Algorithmic fairness and data minimization are basic pillars of the system. The MADRL reward system eliminates attributes such as gender, caste, and religion from the match score. Bias audits are incorporated into the system's governance to detect and address proxy discrimination that might be introduced through other attributes such as postcode.

Data Minimisation. The use of zk-SNARK and selective disclosure achieves the DPDPA 2023 requirement that no party, including the platform operator and the individual, is able to access more personal data than is necessary to facilitate the service transaction.

C. Future Work

The near-future enhancements on the roadmap include: (a) federated learning integration to drive quiet improvements across edge devices without ever transmitting interaction data; (b) implementing a dispute resolution system under the auspices of a decentralized autonomous organization (DAO); (c) adding IoT wearables to the mix, e.g., smartwatch SpO2 and fall detection sensors, to feed real-time health data to the session monitor; and (d) expanding the certification curriculum for caregivers to include advanced nursing skills, effectively positioning the platform as a last-mile network of primary healthcare workers.

IX. CONCLUSION

SevaSetu-ShantamCare is a thoughtful, all-encompassing design that seeks to address India's elder care challenge. The design combines sound engineering with a clear social mission. The move away from centralized data silos to a privacy stack based on blockchain, IPFS, and zk-SNARKs eliminates the data ownership barrier that prevents vulnerable care seekers from fully embracing digital services. At its heart is a Gale-Shapley matcher with a boost of MADRL that provides incredibly fast care allocations in under 200 milliseconds while ensuring stability, fairness, and adaptation to changing preferences on both sides of the market. The vernacular NFT micro-learning module equips rural women with verifiable healthcare gig worker qualifications, which is a structural change with socio-economic benefits that last far longer than any single transaction on the platform. Together, these five pillars a privacy stack, intelligence, trust, education, and safety provide a repeatable, scalable model for how to use

Technology to improve social equity in the developing world

- **Interest Conflicts:** The authors declare that there is no conflict of interest regarding the publication of this paper.
- **Funding Statement:** This research received no external funding.
- **Acknowledgments:** Firstly, we would express our sincere thanks to the management of Vardhaman College of Engineering, Hyderabad for providing us with the right environment and all the facilities required to complete this

project. We also would say thanks to our faculty guide for giving their support continuously, their valuable feedback, and encouragement at all stages while working on this project.

X. REFERENCES

[1] Shatam Care Foundation, “Redefining Elder Care through Technology and Inclusion,” ShatamCare Official Website, 2023.
[2] L. Huang, K. Gupta, and D. Singh, “Emergency response and SOS alert systems in home-based care applications,” in Proc. IEEE Int. Conf. Health Informatics, 2020, pp. 201–208.
[3] S. O. Mohammadi and A. Kalhor, “Privacy-preserving health data management: Architecture and challenges,” in Proc. IEEE Int. Conf. Trust, Privacy and Security in Intelligent Systems and Applications, 2017, pp. 45–52.
[4] R. Sharma and M. Patel, “Digital skill development through offline-accessible learning modules for rural caregivers,” J. Rural Dev., vol. 38, no. 2, pp. 98–115, 2019.
[5] M. Johansen and E. Leroy, “Socio-economic impacts of digital caregiver platforms in emerging economies,” Int. J. Social Economics, vol. 48, no. 9, pp. 1234–1250, 2021.
[6] P. Martínez-García, S. Nguyen, and T. Zhang, “User behaviour and privacy concerns in telecare platforms for the elderly,” J. Med. Syst., vol. 42, no. 7, 2018.
[7] United Nations Department of Economic and Social Affairs, “World Population Ageing 2023: Highlights,” UN, New York, 2023.
[8] Ministry of Statistics and Programme Implementation, “Elderly in India 2021,” Government of India, New Delhi, 2021.
[9] H. Ocheja, B. Flanagan, H. Ueda, and H. Ogata, “Managing lifelong learning records through blockchain,” Res. Pract. Technol. Enhanc. Learn., vol. 14, no. 1, p. 4, 2019.
[10] D. J. Bernstein et al., “BBS Signature Scheme,” W3C Draft Community Group Report, Decentralized Identity Foundation, 2023.
[11] [11] J. Schulman, P. Moritz, S. Levine, M. Jordan, and P. Abbeel, “High-dimensional continuous control using generalised advantage estimation,” in Proc. ICLR, 2016.
[12] [12] A. T. Corbett and J. R. Anderson, “Knowledge tracing: Modeling the acquisition of procedural knowledge,” User Model. User-Adapted Interact., vol. 4, no. 4, pp. 253–278, 1994.
[13] [13] J. Groth, “On the Size of Pairing-Based Non-Interactive Arguments,” in Proc. EUROCRYPT, 2016, pp. 305–326.