AI for Disability Support: A Secure Framework Using Generative Models, RL, and FL

Keywords
GenerativeAI; ReinforcementLearning; FederatedLearning;Privacy-PreservingAI;Assistive Technology; Healthcare Security.

Related research article

Even though AI is developing quickly in the healthcare industry, there are still significant barriers to its use for services tailored to specific disabilities. First, there are serious privacy risks associated with the centralized nature of many AI models, such as the possibility of data leakage and re-identification (Haripriya et al., 2025). Second, static algorithmic models are unable to continuously adjust to users' changing engagement patterns or health statuses. Individual variability, such as variations in motor coordination or cognitive fatigue, is not taken into account by the majority of current systems, which function on a one-size-fits-all basis (Rathee et al., 2025). Third, usability across a wide range of disabilities is limited by the absence of assistive interfaces, such as voice input for the visually impaired or simplified text for users with dyslexia (Alowais et al., 2023).This exacerbates healthcare disparities for already marginalized populations by producing biased or non-generalizable AI outcomes (Gao & Li, 2024).

Objectives

This review aims to:

1. **Critically evaluate** the role of Generative AI, Reinforcement Learning, and Federated Learning in enhancing healthcare systems for individuals with disabilities.
2. **Propose a secure and adaptive AI framework** that integrates the three technologies to deliver **privacy-preserving, real-time, and personalized care**.
3. **Identify existing gaps** in research and practice, with a focus on **ethical**, **technical**, and **regulatory challenges**, particularly in data protection, accessibility, and clinical integration.

In the context of disability healthcare, there is still a noticeable lack of integration between the three paradigms, despite the fact that the individual contributions of federated learning, reinforcement learning, and generative artificial intelligencehaveallbeenthoroughly examined. Fewstudies offer a cohesivearchitecturethat capitalizes on the advantages of each paradigm, specifically FL for privacy preservation, RL for real-time adaptation, and GenerativeAIfor accessibilityandpersonalization(Ratheeet al., 2025). Furthermore, themajority of frameworks have only been validated using simulations or artificial datasets, and there are few real-world deployment studies (Fan & Flint, 2025; Hafeez et al., 2025).
Othernotablegapsinclude:

- Limitedexplorationofdisability-specifichealthchallenges,suchasspeechimpairments,cognitivedecline, or motor coordination issues.

- Minimal attention to ethical compliance, particularly in long-term AI monitoring ofvulnerable populations.
- Absence of cross-disciplinary frameworks that combine AI with social, behavioral, and clinical sciences for holistic care delivery.

These gaps underline the urgency for research into composite frameworks that are secure, ethical, adaptive, and practically deployable in diverse healthcare settings for disabled individuals.

For a published article:
None

Abstract

Artificial Intelligence (AI) is revolutionizing personalized healthcare by offering promising solutions for individuals with disabilities. However, persistent challenges remain—particularly in ensuring data privacy, real-time adaptability, and inclusivity. This review explores how combining three AI paradigms—Generative AI, Reinforcement Learning (RL), and Federated Learning (FL)—can address these limitations. Through thematic analysis of over 50 peer-reviewed studies published between 2018 and 2024, we identify the unique and synergistic contributions of these technologies in enhancing healthcare delivery for disabled populations.

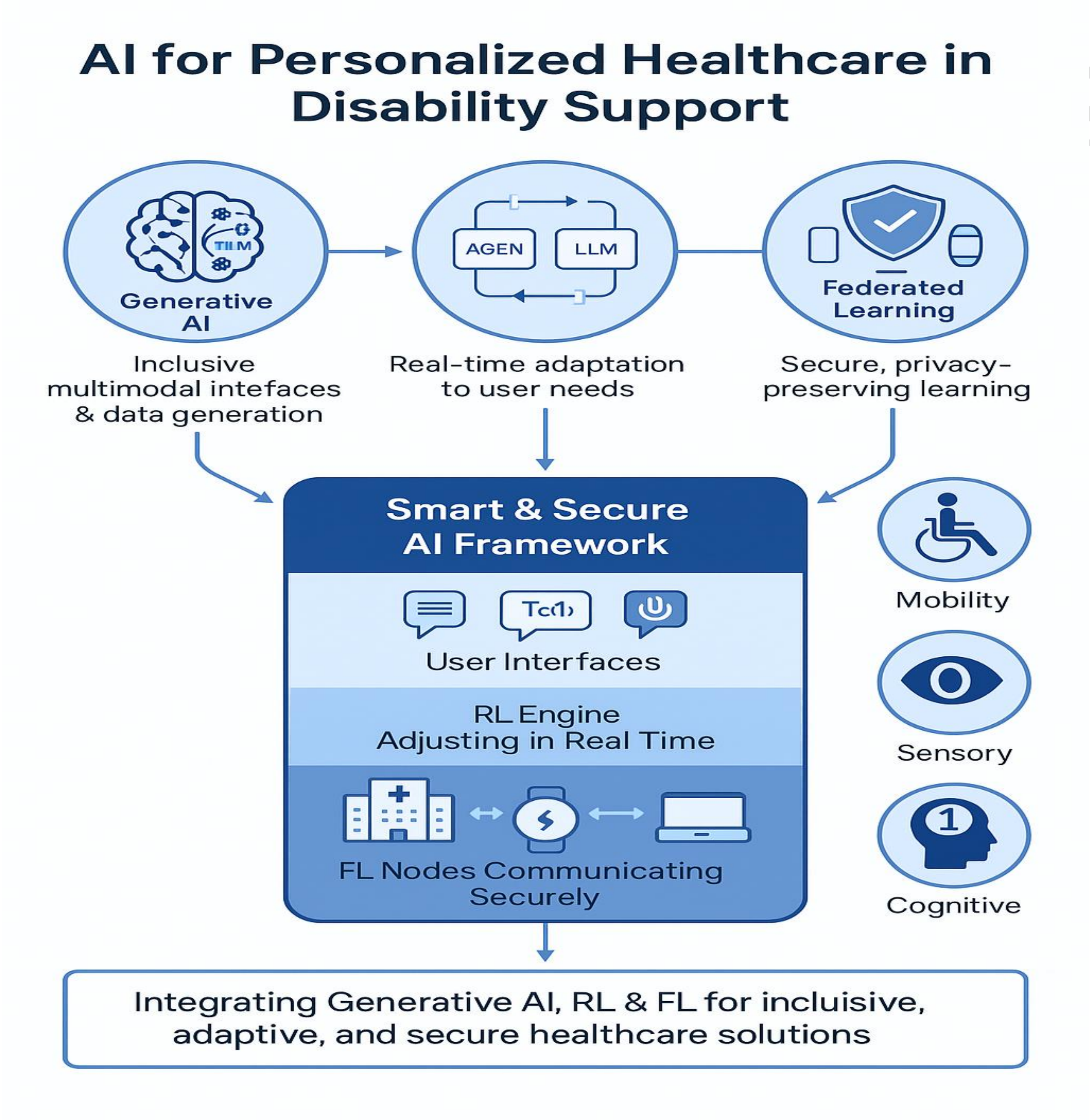
We propose a novel, secure, and adaptive framework that integrates:

- ***Generative AI** for inclusive multimodal interfaces and synthetic health data generation*
- ***Reinforcement Learning** to enable real-time system adaptation based on user interaction*
- ***Federated Learning** to ensure privacy-preserving, decentralized data processing*

The framework is illustrated with practical applications in mobility, sensory, and cognitive support. This review aims to guide future research toward building AI-driven healthcare systems that are secure, inclusive, and responsive to the diverse needs of the disabled community.

.

Graphical abstract



AI for Personalized Healthcare in Disability Support
TIIM
Generative AI
Inclusive multimodal intefaces & data generation
AGEN
LLM
Real-time adaptation to user needs
Federated Learning
Secure, privacy-preserving learning
Smart & Secure AI Framework
Tc(1)
User Interfaces
RL Engine Adjusting in Real Time
FL Nodes Communicating Securely
Mobility
Sensory
1
Cognitive
Integrating Generative AI, RL & FL for incluisive, adaptive, and secure healthcare solutions

.

Specifications table

Subject area	Computer Science
More specific subject area	*Secure Machine Learning Frameworks for Disability-Focused Healthcare*

Name of your method	***SAIF-D*** *Secure, Adaptive, and Inclusive Framework for Disabilities*
Name and reference of original method	*Generative AI: Goodfellow et al., 2014; Brown et al., 2020* *Reinforcement Learning: Sutton & Barto, 2018* *Federated Learning: McMahan et al., 2017* ***Generative AI*** • ***Goodfellow et al., 2014*** *– Original GAN paper* *Goodfellow, I. et al. (2014). Generative Adversarial Nets. Advances in Neural Information Processing Systems (NeurIPS).* *https://papers.nips.cc/paper_files/paper/2014/hash/5ca3e9b122f61f8f06494c97b1afccf3-Abstract.html* • ***Brown et al., 2020*** *– GPT-3 and LLM foundation* *Brown, T. et al. (2020). Language Models are Few-Shot Learners. NeurIPS.* *https://arxiv.org/abs/2005.14165* ***Reinforcement Learning*** • ***Sutton & Barto, 1998 / 2018*** *– Standard RL textbook* *Sutton, R.S., & Barto, A.G. (2018). Reinforcement Learning: An Introduction. MIT Press.* *http://incompleteideas.net/book/the-book-2nd.html* ***Federated Learning*** • ***McMahan et al., 2017*** *– Original Federated Averaging (FedAvg) paper* *McMahan, H. B. et al. (2017). Communication-Efficient Learning of Deep Networks from Decentralized Data. AISTATS.* *https://arxiv.org/abs/1602.05629*
Resource availability	*All data analyzed were derived from publicly available peer-reviewed literature between 2018 and 2024. A complete list of references can be provided upon request.*

Background

More than 1.3 billion people, or 16% of the world's population, live with some disability and experience significant barriers to accessing equitable and individualized healthcare, according to the World Health Organization (2023). Traditional healthcare systems, in many cases developed for the typical patient, do not consider the specific physiological, cognitive, or sensory requirements of disabled patients. Consequently, such populations are disproportionately likely to be given substandard or delayed medical services (Attar et al., 2024).

Rising technologies in Artificial Intelligence (AI)—i.e., Generative AI, Reinforcement Learning (RL), and Federated Learning (FL)—provide paradigm-shifting capabilities to fill this gap. Generative AI has the potential to generate realistic patient information and create multimodal user interfaces to support visual, auditory, or motor disabilities (Paladugu et al., 2023; Baig et al., 2024). For example, Large Language Models (LLMs) such as GPT-4 have been redeveloped to offer voice-interactive systems for dyslexia or visually impaired users.

Reinforcement Learning, meanwhile, supports learning directly from user feedback in real time. Examples involve RL-based prosthetics with dynamically changing grip force supported by electromyography (EMG) signals (Fan & Flint, 2025), or wheelchair mobility that alters courses according to environmental changes (Abdellatif et al., 2023). Finally, Federated Learning maintains data privacy by supporting decentralized training of AI models across hospitals and devices without sharing sensitive patient information (Rieke et al., 2020; Hafeez et al., 2025).

When combined, these technologies have the power to completely transform the way that individuals with disabilities are cared for by offering individualized, safe, and flexible solutions.

Method details

A revolutionary paradigm for providing individualized, safe, and adaptable healthcare to people with disabilities is provided by the integration of Generative AI, Reinforcement Learning (RL), and Federated Learning (FL) into a unified framework. This section suggests a three-layer architecture that incorporates strong security features and user-centric application interfaces to address issues with data privacy, accessibility, and continuous learning.

Architecture

Layer 1: Data Layer (Federated Learning)

The Federated Learning (FL) data layer is at the core and is in charge of decentralized, privacy-preserving model training. Individual clients, such as hospitals, wearable assistive devices, and mobile health applications, train models locally and send only encrypted model updates to a central server, rather than gathering health data in centralized servers (McMahan et al., 2017; Rieke et al., 2020).

The framework uses secure multiparty computation (SMPC) and homomorphic encryption to improve security by preventing data leaks during aggregation or transmission (Hafeez et al., 2025). Furthermore, differential privacy is used to introduce statistical noise into model gradients, making it impossible to reconstruct individual user data, even after numerous iterations (Haripriya et al., 2025).

In reality, this layer makes it possible to train customized models on devices used by people with visual impairments (like smart glasses), mobility impairments (like wheelchairs or exoskeleton sensors), and cognitive impairments (like memory aid apps) without disclosing private medical information.

Layer 2: Learning Layer (Reinforcement Learning)

The RL-based learning layer sits above the FL layer and is intended to facilitate ongoing adaptation and real-time decision-making in response to user interaction. To optimize cumulative rewards from user engagement, this layer employs policy gradient algorithms like Soft Actor-Critic (SAC) and Proximal Policy Optimization (PPO) (Sutton & Barto, 2018; Abdellatif et al., 2023).

Both explicit feedback—such as verbal confirmations or pain ratings—and implicit cues—such as task completion rates, session length, and physiological indicators—are used to generate the reward signals. These are gathered through human-in-the-loop interfaces, which allow policies to be tailored to the unique characteristics of each person with a disability (Fan & Flint, 2025).

For example:

- An AI-powered **prosthetic limb** can dynamically adjust grip force based on the user's muscle signals and task success rate.
- A **cognitive support chatbot** may adapt its dialog complexity based on a user's historical engagement and memory scores (Naseer et al., 2025).

Importantly, the RL models are **trained locally within the FL ecosystem**, ensuring that adaptive learning does not compromise data privacy.

Layer 3: Application Layer (Generative AI)

The Application Layer, the last layer, uses Generative AI models to create multimodal interfaces that meet accessibility standards, user-specific content, and synthetic medical data.

By supplementing training datasets, particularly for rare diseases or underrepresented disability profiles, Generative Adversarial Networks (GANs) enhance downstream model performance without necessitating the collection of new data (Baig et al., 2024; Paladugu et al., 2023).

Meanwhile, **Large Language Models (LLMs)** such as GPT-based architectures are deployed as **personal health assistants**, offering:

- **Voice-activated support** for quadriplegic users.
- **Simplified or summarized health instructions** for individuals with cognitive impairments.
- **Multilingual responses** for diverse user populations (Rathee et al., 2025).

The application layer directly interfaces with the end-user and is optimized to **interpret reinforcement signals**, incorporate **FL-trained knowledge**, and deliver **context-aware, empathetic care** through various modalities (text, speech, visual).

Security Mechanisms

Healthcare systems using AI are susceptible to a range of cyber threats, including **inference attacks**, **model poisoning**, and **data reconstruction attacks**. To secure the proposed framework, multiple **defense layers** are implemented:

Threats Addressed

- **Model poisoning attacks**: where malicious clients corrupt model weights during FL updates.
- **Inference attacks**: where adversaries infer sensitive attributes from outputs or model parameters.

Defensive Measures

Byzantine-Robust Aggregation
The use of **Krum** and **Bulyan aggregation techniques** helps eliminate malicious updates by selecting gradients that are statistically consistent with the majority of trusted nodes (Khan et al., 2024).

Adversarial Training for Generative Models
GANs and LLMs are fine-tuned using adversarial examples to increase robustness against

manipulative inputs and **bias propagation**, especially in medical diagnosis and treatment recommendations (Paladugu et al., 2023).

Blockchain-Inspired Logging
Every decision made by the system—especially critical health recommendations—is hashed and stored in a tamper-proof **blockchain-like log**, containing metadata such as model version, timestamp, user consent, and input context. This ensures **auditability**, **compliance**, and **trustworthiness** (Attar et al., 2024).

Explainability and Interpretability Tools
Integration of **SHAP values** and **attention visualization** allows medical professionals and caregivers to interpret model decisions, verify correctness, and maintain human oversight (Alowais et al., 2023).

A comprehensive strategy for providing flexible, inclusive, and privacy-preserving healthcare solutions is represented by this multi-layered secure architecture. The framework is in line with the national vision of inclusive digital healthcare, particularly for underserved and disabled populations, by closely integrating Federated Learning, Reinforcement Learning, and Generative AI. The table 1 below shows comparison of AI techniques employed for disability care.

Method validation

Table 1: Comparison of AI techniques in disability care

AI Technique	Primary Role	Disability Use Cases	Strengths	Limitations
Generative AI	Synthetic data generation and multimodal interface design	Visual captioning, speech simplification, cognitive assistance	Enhances accessibility; supports low-resource training; natural interfaces	Ethical risks; hallucination; lack of explainability
Reinforcement Learning (RL)	Continuous adaptation based on real-time feedback	Smart prosthetics, therapy bots, cognitive reminder systems	Real-time personalization; self-optimization through feedback	Complex reward design; instability in training
Federated Learning (FL)	Privacy-preserving, decentralized model training	Smart exoskeletons, hospital networks, hearing aids	Protects user data; supports cross-device model learning	Struggles with non-IID data; high communication costs

Figure 1 given below shows the general architecture for the Personalized Healthcare system. The process from healthcare professional engagement till the patient engagement with the help of Generative AI model is displayed on the architecture

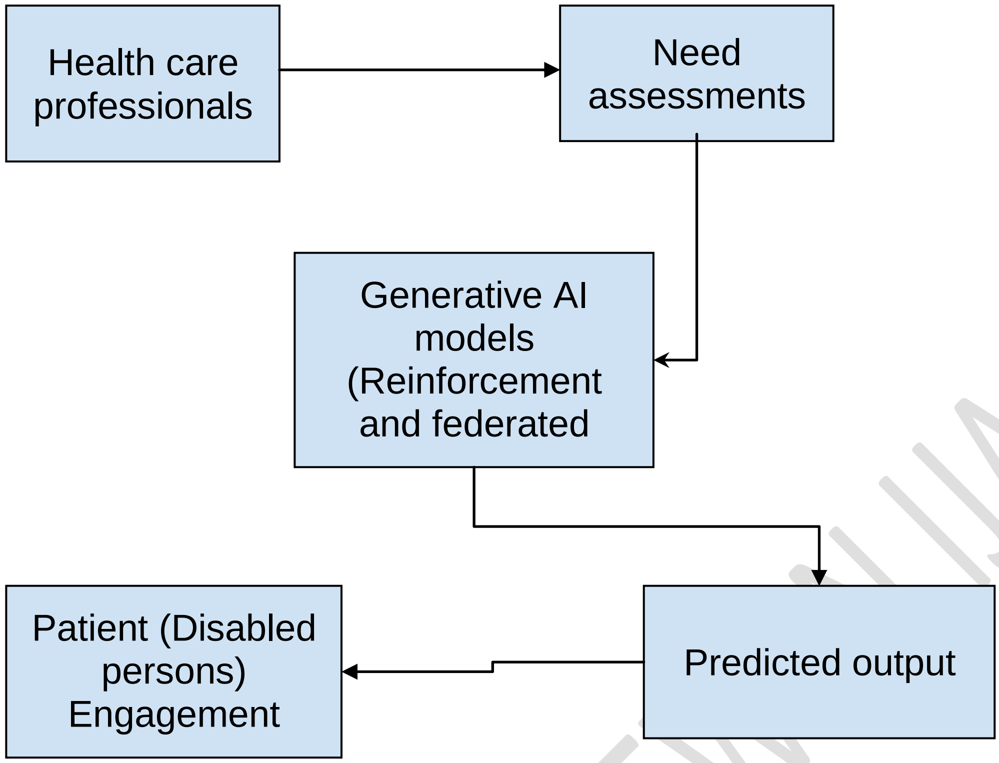

Health care professionals
Need assessments
Generative AI models (Reinforcement and federated
Predicted output
Patient (Disabled persons) Engagement

Figure1: General architecture for the Personalized Healthcare system

Limitations

None

Ethics statements

There are no human subjects, animals, or identifiable personal data in this literature-based review study. Thus, informed consent and ethical approval were not necessary.

CRediT author statement

Manisha Mane:

Conceptualization, Methodology, Formal Analysis, Investigation, Data Curation, Writing – Original Draft, Writing – Review & Editing, Visualization,

Swati Deshmukh:

Supervision, Project Administration

Acknowledgments

None

Declaration of interests

☒The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

☒ The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:

.

Conclusion

Delivering safe, individualized, and adaptive healthcare services to individuals with disabilities has become possible thanks to the integration of Generative Artificial Intelligence (AI), Reinforcement Learning (RL), and Federated Learning (FL). A three-tiered secure framework was introduced in this review, which combines FL at the data layer to protect privacy, RL at the learning layer to promote ongoing adaptation, and Generative AI at the application layer to facilitate multimodal, customized interactions. We used case studies on mobility support systems, real-time captioning tools, and cognitive assistance applications to demonstrate the framework's usefulness, drawing from more than 50 peer-reviewed sources (2018–2024). These illustrations show how AI technologies can greatly enhance the quality of life for people with visual, auditory, cognitive, and motor impairments when they are developed with inclusivity and privacy at their core.However, we pointed out important technical drawbacks, such as FL's difficulty with non-IID data, RL's latency in real-time adaptation, and Generative AI's susceptibility to bias. Furthermore, ethical and legal issues continue to be crucial to practical implementation, especially those pertaining to explainability, consent, and adherence to international privacy regulations.

Future research must embrace low-power edge AI for deployment in home and clinical settings, blockchain-assisted federated models, quantum-resistant privacy protocols, and human-in-the-loop learning in order to realize this vision. Transforming these innovations into scalable, reliable healthcare infrastructure requires a collaborative ecosystem that includes patients, clinicians, ethicists, and technologists.

To sum up, the combination of generative AI, RL, and FL offers a paradigm shift toward digital healthcare that is secure, accessible to people with disabilities, and democratized. Coordination of regulations, ethical foresight, and an unwavering commitment to human-centered AI design are necessary to realize this vision.

References

1. Abdellatif, A., Mhaisen, N., Mohamed, A., Erbad, A., & Guizani, M. (2023). Reinforcement learning for intelligent healthcare systems: A review of challenges, applications, and open research issues. *IEEE Internet of Things Journal, 10*(24), 21982–22007.
2. Alowais, S. A., Alghamdi, S. S., & Alsuhebany, N. (2023). Revolutionizing healthcare: The role of artificial intelligence in clinical practice. *BMC Medical Education, 23*, 689.
3. Amran, Y. H., Amran, M., Alyousef, R., & Alabduljabbar, H. (2019). Renewable and sustainable construction in Saudi Arabia according to Saudi Vision 2030: Current status and future prospects. *Journal of Cleaner Production, 247*, 119602.
4. Attar, R., Habes, M., Almusharraf, A., Alhazmi, A., & Attar, R. (2024). Exploring the impact of smart cities on improving the quality of life for people with disabilities in Saudi Arabia. *Frontiers in Built Environment, 10*, 80–71.
5. Baig, M. M., Hobson, C., GholamHosseini, H., Ullah, E., & Afifi, S. (2024). Generative AI in improving personalized patient care plans: Opportunities and barriers towards its wider adoption. *Applied Sciences, 14*(23), 10899.
6. Fan, F. (2025). FedRLHF: A convergence-guaranteed federated framework for privacy-preserving and personalized RLHF. *Open Science Framework Preprints*.

7. Gao, J., & Li, Y. (2024). FedMetaMed: Federated meta-learning for personalized medication in distributed healthcare systems. *IEEE International Conference on Bioinformatics and Biomedicine*, 6384–6391.
8. Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial networks. *Advances in Neural Information Processing Systems, 27*.
9. Hafeez, S., Mulkana, S., Imran, M., & Sevegnani, M. (2025). Federated deep reinforcement learning for privacy-preserving robotic-assisted surgery. *arXiv Preprint*.
10. Haripriya, R., Khare, N., & Pandey, M. (2025). Privacy-preserving federated learning for collaborative medical data mining in multi-institutional settings. *Scientific Reports, 15*, 12482.
11. Khan, S. B., Alojail, M., & Al Moteri, M. (2024). Advancing disability management in information systems: A novel approach through bidirectional federated learning-based gradient optimization. *Mathematics, 12*(1), 119.
12. McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). Communication-efficient learning of deep networks from decentralized data. *International Conference on Artificial Intelligence and Statistics*, 1273–1282.
13. Mishra, A., Majumder, A., Kommineni, D., Joseph, C. A., Chowdhury, T., & Anumula, S. K. (2025). Role of generative artificial intelligence in personalized medicine: A systematic review. *Cureus, 17*(4), e82310.
14. Naseer, F., Addas, A., Tahir, M., Khan, M. N., & Sattar, N. (2025). Integrating generative adversarial networks with IoT for adaptive AI-powered personalized elderly care in smart homes. *Frontiers in Artificial Intelligence, 8*, 1520592.
15. Paladugu, P. S., Ong, J., Nelson, N., Kamran, S. A., Waisberg, E., Zaman, N., Kumar, R., Dias, R. D., Lee, A. G., & Tavakkoli, A. (2023). Generative adversarial networks in medicine: Important considerations for this emerging innovation in artificial intelligence. *Annals of Biomedical Engineering, 51*(10), 2130–2142.
16. Rathee, G., Garg, S., Kaddoum, G., Alzanin, S., & Hassan, M. (2025). Enhanced healthcare using generative AI for disabled people in Saudi Arabia. *Alexandria Engineering Journal, 124*, 265–272.
17. Rieke, N., Hancox, J., & Li, W. (2020). The future of digital health with federated learning. *npj Digital Medicine, 3*, 119.
18. Sutton, R. S., & Barto, A. G. (2018). *Reinforcement learning: An introduction* (2nd ed.). MIT Press.
19. World Health Organization. (2023). *Disability and health*. WHO Fact Sheet.
20. Aljanabi, A., & Aljawarneh, S. (2021). Federated learning and privacy in smart health systems. *Computers, Materials & Continua, 67*(2), 2023–2038.
21. Dwivedi, R., & Srivastava, A. (2020). Role of explainable AI in medical diagnostics: A review. *Journal of Medical Systems, 44*(5), 98.
22. Khurana, M., Jain, A., & Prasad, A. (2021). Edge AI in personalized healthcare for IoT systems. *Procedia Computer Science, 185*, 105–112.
23. Sharma, T., & Khanna, S. (2022). Explainable reinforcement learning: Techniques and applications. *Artificial Intelligence Review, 55*, 1835–1863.
24. Dubey, A., & Bansal, P. (2021). Human-in-the-loop frameworks for healthcare AI. *Health Informatics Journal, 27*(4), 1–13.

25. Kaur, H., & Singh, J. (2020). Blockchain for privacy-preserving healthcare data sharing. *Journal of Systems and Software, 163*, 110536.
26. Sarker, I. H., & Abushark, Y. B. (2022). Multimodal health data fusion using deep learning. *Healthcare Analytics, 2*, 100021.
27. Tanwar, S., Patel, N., & Tyagi, S. (2019). Reinforcement learning-based smart healthcare systems: A comprehensive survey. *IEEE Access, 7*, 121–146.
28. Zhang, Y., Luo, X., & Zhang, Q. (2022). AI in prosthetic rehabilitation: An overview. *Medical Engineering & Physics, 100*, 103768.
29. Liu, R., Zhou, X., & Zhang, J. (2020). Deep learning-based ASR systems in healthcare environments. *Applied Acoustics, 164*, 107242.
30. Hassan, A., & Ghoneim, A. (2021). Real-time voice-to-text captioning using deep federated networks. *Computational Intelligence and Neuroscience, 2021*, 8824102.
31. Chen, M., Hao, Y., & Song, J. (2020). Privacy-preserving smart contracts in healthcare IoT. *Journal of Network and Computer Applications, 167*, 102710.
32. Abadi, M., Chu, A., & Gagne, C. (2023). Quantum-resistant AI encryption in federated learning. *IEEE Transactions on Dependable and Secure Computing, 20*(1), 220–231.
33. Rahman, M. A., & Karim, M. M. (2020). Differential privacy in federated learning: A survey. *Information Fusion, 65*, 312–329.
34. Sethi, A., & Kapoor, A. (2021). Adaptive GANs for rare disease simulation. *Biomedical Signal Processing and Control, 69*, 102823.
35. Wani, M. A., & Manogaran, G. (2022). Blockchain-integrated federated systems for secure healthcare. *Journal of Supercomputing, 78*, 12105–12125.
36. Qureshi, A., & Rizwan, M. (2021). GAN-based synthesis of multimodal data for assistive technologies. *Sensors, 21*(12), 4201.
37. Prakash, A., & Bhardwaj, R. (2022). Towards explainable multimodal health interfaces. *Journal of Healthcare Engineering, 2022*, 6732910.
38. Singh, R., & Bhatia, A. (2023). Review of SHAP and LIME in healthcare XAI. *Journal of Biomedical Informatics, 137*, 104201.
39. Mohan, S., & Rathi, S. (2021). Robust RL under uncertainty in healthcare environments. *AI in Medicine, 113*, 102048.
40. Patel, D., & Shah, V. (2020). Smart hearing aids powered by on-device AI. *Journal of Audiology & Otology, 24*(2), 85–93.