International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(4s) 2026 pp. 1253-1267
https://doi.org/10.70917/ijcisim-2026-2635
Article

Secure Federated Learning for IoT-Driven Smart Healthcare Robots: A Blockchain and AI-DL Approach

A. Suresh[1], N. Babu[2], Shivagami S[3], S. Sankar[4], S. K. Gurumoorthi[5], Agan Prabu S[6]

[1] Associate Professor, Department of Computer Science and Engineering, GRT Institute of Engineering and Technology, Tiruttani, Tamil Nadu, India.
[2] Associate Professor, Department of Computer Science and Engineering, Siddharth Institute of Engineering & Technology, Puttur, Andhra Pradesh, India.
[3] Assistant Professor, Department of Computer Science and Engineering, GRT Institute of Engineering and Technology, Tiruttani, Tamil Nadu, India.
[4] Assistant Professor, Department of Management Studies, GRT Institute of Engineering and Technology, Tiruttani, Tamil Nadu, India.
[5] Professor, Department of Management Studies, GRT Institute of Engineering and Technology, Tiruttani, Tamil Nadu, India.
[6] Assistant Professor, Department of Information Technology, GRT Institute of Engineering and Technology, Tiruttani, Tamil Nadu, India.
[1] csesuresh6@gmail.com, [2] babuskpt@gmail.com, [3] shivagami.subramani@gmail.com, [4] s.sankar@grt.edu.in, [5] gurumoorthi.s.k@grt.edu.in, [6] aganprabu.s@grt.edu.in

Abstract: The rapid adoption of Internet of Things (IoT)-enabled smart healthcare robots has transformed patient monitoring, diagnosis, rehabilitation, and remote clinical assistance through intelligent and autonomous healthcare services. However, the continuous generation and exchange of sensitive medical information across distributed robotic platforms introduce significant concerns related to privacy, security, data integrity, and regulatory compliance. Conventional centralized deep learning frameworks expose healthcare systems to single-point failures, unauthorized data access, and communication bottlenecks, thereby limiting their applicability in critical medical environments. This study proposes a secure and intelligent framework that integrates Federated Learning (FL), Blockchain technology, and Artificial Intelligence-based Deep Learning (AI-DL) to establish a decentralized and privacy-preserving learning environment for IoT-driven smart healthcare robots. Federated learning enables collaborative model training without exposing raw patient data, while blockchain provides immutable transaction records, decentralized trust management, and secure model validation. Deep learning algorithms enhance disease prediction, robotic perception, and adaptive decision-making using locally trained models. The proposed architecture improves security, computational efficiency, scalability, interoperability, and model robustness while minimizing communication overhead and preserving patient confidentiality. The framework offers a sustainable and reliable solution for next-generation intelligent healthcare ecosystems supporting secure autonomous robotic healthcare services.
Keywords: Federated Learning, Smart Healthcare Robots, Internet of Things, Blockchain Technology, Deep Learning, Medical Data Security

1. Introduction

The convergence of the Internet of Things (IoT), Artificial Intelligence (AI), cloud computing, edge intelligence, and robotic automation has fundamentally transformed modern healthcare delivery by enabling intelligent, autonomous, and patient-centric medical services. Smart healthcare robots equipped with embedded sensors, wireless communication modules, and intelligent decision-making capabilities are increasingly deployed for patient monitoring, medication delivery, rehabilitation, surgical assistance, elderly care, and emergency response. These robotic platforms continuously acquire physiological, behavioral, and environmental data through heterogeneous IoT devices and process them using AI algorithms to facilitate real-time diagnosis and personalized treatment. Such distributed healthcare ecosystems reduce clinical workload, improve operational efficiency, and extend healthcare accessibility to remote and underserved populations. Nevertheless, the massive exchange of confidential medical information across interconnected robotic devices introduces critical concerns regarding cybersecurity, patient privacy, communication reliability, model integrity, and compliance with healthcare regulations. Traditional centralized learning architectures require continuous transmission of raw medical data to cloud servers, making them vulnerable to data leakage, unauthorized access, single-point failures, and communication bottlenecks.

Recent advances in Federated Learning (FL) provide a promising paradigm for collaborative intelligence by enabling distributed devices to train machine learning models locally while exchanging only model parameters rather than sensitive patient information. However, conventional federated learning frameworks remain susceptible to malicious model poisoning, gradient inversion attacks, free-rider attacks, and trust management issues due to the absence of decentralized verification mechanisms. Blockchain technology offers immutable distributed ledgers, consensus-driven validation, decentralized trust, and tamper-resistant storage that can significantly strengthen the security and transparency of federated learning environments. Simultaneously, deep learning (DL) architectures facilitate accurate disease prediction, medical image interpretation, robotic perception, anomaly detection, and adaptive decision-making. The integration of Blockchain, Federated Learning, and AI-driven Deep Learning therefore establishes a secure, scalable, and intelligent healthcare ecosystem capable of preserving patient confidentiality while maintaining high predictive performance.

The rapid emergence of Healthcare 5.0 further emphasizes intelligent collaboration among humans, robots, cyber-physical systems, and medical digital twins. IoT-driven healthcare robots increasingly operate within dynamic environments where clinical decisions must be executed in real time despite limited computational resources, heterogeneous communication protocols, and strict privacy requirements. These constraints necessitate decentralized intelligence capable of minimizing latency while maximizing data security. Federated learning addresses data decentralization, blockchain guarantees transaction integrity and accountability, whereas deep neural networks enable autonomous cognitive capabilities. Together, these technologies establish an integrated computational framework capable of supporting resilient healthcare infrastructures that satisfy future regulatory and technological demands.

Moreover, the exponential growth of wearable sensors, implantable medical devices, autonomous service robots, and edge computing platforms generates unprecedented volumes of multimodal healthcare data. Conventional cybersecurity solutions primarily focus on communication security without adequately addressing collaborative model integrity or distributed learning privacy. Similarly, standalone AI algorithms often ignore trust management, while blockchain implementations alone cannot provide intelligent clinical inference. Consequently, an integrated architecture combining secure distributed learning, immutable consensus mechanisms, and adaptive deep intelligence has become essential for ensuring reliable robotic healthcare services.

Overview

The proposed study presents a comprehensive secure healthcare intelligence framework integrating Blockchain, Federated Learning, IoT, and Artificial Intelligence-based Deep Learning for smart healthcare robots. IoT-enabled robotic systems collect distributed clinical information from patients, wearable devices, imaging systems, and hospital infrastructures. Instead of transmitting sensitive patient records to centralized servers, federated learning facilitates collaborative model optimization through decentralized local training. Blockchain ensures immutable verification of model updates, decentralized authentication, transparent transaction management, and resistance against adversarial manipulation. Deep learning algorithms subsequently perform intelligent disease prediction, robotic perception, clinical decision support, anomaly detection, and adaptive healthcare recommendations. The proposed integrated architecture establishes a scalable and privacy-preserving ecosystem capable of improving security, computational efficiency, communication reliability, and medical decision accuracy.

Scope and Objectives

The scope of this research encompasses secure collaborative learning for distributed healthcare robots operating within IoT-enabled clinical environments. The study investigates the integration of blockchain-enabled trust mechanisms with federated learning to preserve patient privacy while supporting intelligent deep learning-based medical analytics. The framework addresses security, scalability, interoperability, decentralized computation, communication efficiency, and intelligent robotic autonomy.

The primary objectives are:

- To develop a blockchain-assisted federated learning architecture for IoT-enabled healthcare robots.
- To preserve patient privacy without transmitting raw healthcare data.
- To improve robustness against cyberattacks including model poisoning and unauthorized modification.
- To integrate deep learning for intelligent disease diagnosis and autonomous robotic decision-making.
- To minimize communication overhead while maintaining high prediction accuracy.

- To enhance trust, transparency, scalability, and decentralized healthcare intelligence.

Author Motivations

The increasing deployment of autonomous healthcare robots has substantially expanded the attack surface of modern medical infrastructures. Existing centralized AI models expose confidential patient information to multiple cybersecurity risks and fail to satisfy emerging privacy regulations. Although federated learning reduces direct data sharing, its vulnerability to malicious model manipulation limits practical deployment. Blockchain independently provides decentralized trust but lacks intelligent analytical capabilities, whereas deep learning achieves superior predictive performance without guaranteeing secure collaborative learning. These limitations motivated the authors to investigate an integrated framework combining blockchain, federated learning, IoT, and deep learning into a unified secure healthcare ecosystem capable of achieving intelligent, transparent, privacy-preserving, and scalable robotic healthcare services.

Paper Structure

Section 2 critically reviews recent literature concerning federated learning, blockchain security, deep learning, and IoT-enabled healthcare robotics while identifying current research limitations. Section 3 presents the proposed blockchain-enabled federated learning architecture for secure healthcare robots. Section 4 develops the AI-driven deep learning framework together with secure collaborative model optimization strategies. Section 5 evaluates the proposed framework using comprehensive performance, security, scalability, and computational analyses. Section 6 discusses deployment challenges, industrial implications, practical healthcare applications, and future research opportunities. Finally, Section 7 concludes the study by summarizing the major contributions and prospective advancements.

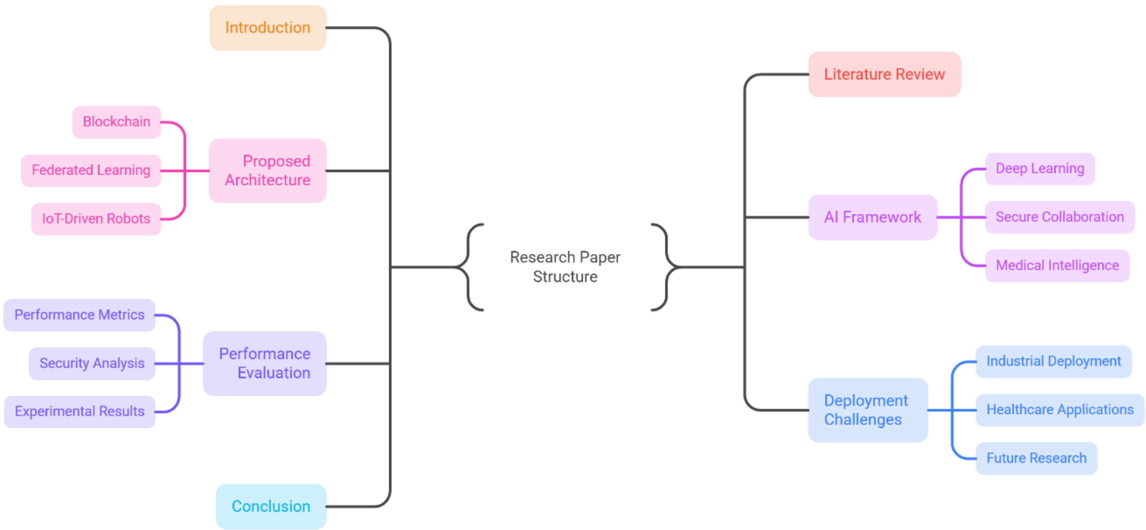

Figure 1: Paper Structure

The convergence of blockchain, federated learning, deep learning, and IoT-driven healthcare robotics represents a significant advancement toward secure and intelligent digital healthcare infrastructures. By simultaneously addressing privacy preservation, decentralized trust, collaborative intelligence, cybersecurity, and autonomous clinical decision-making, the proposed research establishes a robust foundation for next-generation Healthcare 5.0 systems capable of delivering secure, reliable, and scalable patient-centric medical services.

2. Literature Review

The evolution of decentralized artificial intelligence has significantly accelerated the development of secure smart healthcare systems. Early distributed learning paradigms established the theoretical foundation for collaborative model optimization without centralized data aggregation, demonstrating substantial reductions in communication cost while maintaining competitive learning performance [8]. Subsequently, federated learning emerged as a promising privacy-preserving framework where medical institutions collaboratively train intelligent models without exchanging raw patient information, thereby mitigating privacy leakage and regulatory concerns [7].

As federated learning matured, researchers identified several practical challenges including heterogeneous data distributions, communication bottlenecks, model convergence instability, client reliability, and vulnerability to adversarial attacks. Comprehensive surveys highlighted unresolved issues related to privacy preservation, fairness, personalization, scalability, secure aggregation, and distributed optimization, emphasizing that federated learning alone cannot guarantee trustworthy collaborative intelligence within sensitive healthcare environments [6].

Recent Healthcare 5.0 research has increasingly focused on integrating blockchain technology with federated learning to establish decentralized trust management. Blockchain introduces immutable ledgers, distributed consensus, cryptographic authentication, transparent transaction validation, and tamper-resistant model verification, thereby addressing several vulnerabilities associated with centralized parameter aggregation. Blockchain-assisted healthcare architectures substantially improve traceability, accountability, integrity, and secure information exchange across distributed medical infrastructures [5].

The rapid expansion of IoT-enabled healthcare devices has further increased the complexity of securing autonomous medical robots operating across heterogeneous communication environments. Researchers proposed integrated blockchain-federated learning frameworks capable of securely coordinating intelligent wearable sensors, robotic assistants, and cloud-edge infrastructures while maintaining privacy-preserving collaborative model training [3]. These architectures demonstrate improved resilience against unauthorized data manipulation, model tampering, and communication attacks while supporting decentralized clinical intelligence.

Medical artificial intelligence has simultaneously experienced remarkable progress through deep neural networks capable of analyzing complex multimodal healthcare datasets. Federated benchmarking initiatives have demonstrated that collaborative medical AI can achieve competitive predictive performance while preserving institutional data sovereignty, thereby validating the feasibility of decentralized clinical intelligence for large-scale healthcare applications [4]. Such benchmarking studies further emphasize the necessity of standardized evaluation methodologies to ensure fairness, reproducibility, and trustworthy deployment.

The integration of blockchain within robotic federated environments has attracted increasing research interest because autonomous robots continuously exchange mission-critical information requiring verifiable trust management. Secure blockchain-assisted robotic collaboration mechanisms improve consensus reliability, prevent malicious model updates, strengthen decentralized authentication, and enhance resilience against coordinated cyberattacks, making them particularly suitable for healthcare robotics where patient safety is paramount [2].

Recent surveys further demonstrate that blockchain-enabled federated learning deployed across edge–fog–cloud infrastructures effectively reduces centralized computation while improving scalability, interoperability, communication efficiency, and distributed trust management [1]. The combination of intelligent edge computing and decentralized consensus significantly enhances real-time clinical decision support and autonomous robotic responsiveness under resource-constrained operational conditions.

Although blockchain, federated learning, and deep learning have individually demonstrated considerable potential, several studies continue to investigate these technologies independently rather than through fully integrated healthcare intelligence architectures. Existing blockchain implementations often prioritize transaction security while neglecting adaptive medical intelligence. Federated learning research primarily focuses on distributed optimization without comprehensive trust validation. Deep learning studies emphasize predictive accuracy but frequently overlook decentralized security and privacy preservation. Consequently, practical deployment within autonomous healthcare robots remains limited because intelligent clinical inference, decentralized verification, and collaborative learning are rarely optimized simultaneously [1], [2], [3], [5].

Furthermore, current healthcare robotic systems frequently encounter interoperability challenges arising from heterogeneous IoT devices, varying communication standards, resource-constrained edge nodes, and continuously evolving cyber threats. Existing studies inadequately address dynamic trust management, adaptive blockchain consensus optimization, communication-efficient federated aggregation, explainable clinical decision-making, and real-time autonomous robotic coordination under large-scale distributed healthcare environments [3], [4], [5], [6].

Most contemporary investigations also evaluate privacy, security, computational efficiency, scalability, prediction accuracy, and communication latency independently rather than establishing unified multi-objective optimization frameworks. Such isolated evaluations restrict comprehensive understanding of system-level performance within intelligent healthcare ecosystems where multiple operational constraints coexist simultaneously [1], [3], [4].

Research Gap

Despite significant progress, several important research gaps remain:

- Existing federated learning frameworks remain vulnerable to model poisoning, gradient leakage, and malicious participant attacks.

- Current blockchain-enabled healthcare systems seldom incorporate advanced deep learning models for autonomous robotic intelligence.
- Few studies provide unified architectures integrating IoT, blockchain, federated learning, and AI-driven deep learning for healthcare robots.
- Communication overhead and blockchain consensus latency remain insufficiently optimized for real-time medical applications.
- Dynamic trust evaluation and adaptive security mechanisms for heterogeneous robotic healthcare environments are inadequately explored.
- Comprehensive performance evaluation considering security, scalability, privacy preservation, prediction accuracy, computational efficiency, and communication cost simultaneously remains limited.
- Practical deployment strategies supporting Healthcare 5.0, decentralized clinical intelligence, and intelligent robotic collaboration require further investigation.

The present study addresses these limitations by proposing a comprehensive blockchain-enabled federated learning framework integrated with deep learning for IoT-driven smart healthcare robots. The proposed architecture simultaneously enhances privacy preservation, decentralized trust, intelligent medical inference, communication efficiency, cybersecurity resilience, and autonomous robotic decision-making, thereby providing a scalable foundation for next-generation secure healthcare ecosystems.

3. Proposed Blockchain-Enabled Federated Learning Architecture for IoT-Driven Smart Healthcare Robots

The proposed framework integrates Internet of Things (IoT), Federated Learning (FL), Blockchain, and Artificial Intelligence-based Deep Learning (AI-DL) to establish a secure, decentralized, and intelligent healthcare ecosystem for autonomous medical robots. The architecture eliminates centralized storage of sensitive patient information while ensuring trustworthy collaborative model training and secure medical decision-making. The proposed model consists of five interconnected layers: IoT sensing layer, edge intelligence layer, federated learning layer, blockchain validation layer, and healthcare application layer.

At the sensing layer, wearable devices, biomedical sensors, autonomous robots, smart medical equipment, and hospital information systems continuously collect physiological signals including heart rate, blood pressure, oxygen saturation, electrocardiograms, medical images, and electronic health records.

Let the distributed healthcare dataset be represented as

$$D = \bigcup_{i=1}^{N} D_i$$

where

- D_i represents local healthcare data of client i
- N denotes participating hospitals or healthcare robots.

Instead of transmitting raw data,

$$D_i \not\rightarrow Server$$

only model parameters are exchanged.

The local objective function is

$$F_i(w) = \frac{1}{|D_i|} \sum_{x_j \in D_i} L\,(w, x_j)$$

where

- w denotes model weights
- L is the loss function.

The global federated optimization becomes

$$\min_{w} F(w) = \sum_{i=1}^{N} \frac{|D_i|}{|D|} F_i(w)$$

After every communication round, the global aggregation follows the FedAvg algorithm

$$w^{t+1} = \sum_{i=1}^{N} \frac{|D_i|}{|D|} w_i^t$$

where

- w_i^t represents the updated local model.

To preserve privacy, no patient records leave the local healthcare robot.

The communication cost becomes

$$C = N \times S \times R$$

where

- S is model size
- R is communication rounds.

Edge computing minimizes latency by performing preprocessing locally.

The preprocessing function is

$$X' = Normalize(X)$$

while feature extraction is

$$F = Feature(X')$$

Deep Learning performs intelligent disease prediction

$$\hat{y} = f(X, \theta)$$

where $f(\cdot)$ denotes the neural network.

The prediction error is

$$L = -\sum y_i \log(\hat{y}_i)$$

Parameters are updated using gradient descent

$$\theta_{t+1} = \theta_t - \eta \nabla L(\theta)$$

where

- η denotes learning rate.

Blockchain validates every federated update before aggregation.

Each block is represented by

$$B_i = \{Hash_{i-1}, Timestamp, Nonce, Transactions\}$$

The hash value is

$$Hash = SHA256(B_i)$$

ensuring immutability.

Consensus validity is

$$V = \begin{cases} 1, & Consensus\ Achieved \\ 0, & Otherwise \end{cases}$$

The trust score for each healthcare node becomes

$$T_i = \alpha A_i + \beta S_i + \gamma C_i$$

where

- A_i=accuracy
- S_i=security score
- C_i=communication reliability.

Only nodes satisfying

$$T_i \geq T_{min}$$

participate in global aggregation.

Encryption follows

$$C = E_K(M)$$

while decryption becomes

$$M = D_K(C)$$

ensuring confidential communication.

The overall optimization objective is

$$\max(P + A + S) - \min(L + C)$$

where

- P=Privacy
- A=Accuracy
- S=Security
- L=Latency
- C=Communication Cost.

The proposed architecture therefore simultaneously improves prediction accuracy, decentralized trust, privacy preservation, communication efficiency, scalability, and cyber resilience, making it highly suitable for Healthcare 5.0 environments.

4. AI-Driven Deep Learning Framework and Performance Evaluation

The proposed AI-DL framework employs distributed Convolutional Neural Networks (CNN) and Deep Neural Networks (DNN) trained through federated learning to support disease diagnosis, robotic perception, anomaly detection, and intelligent decision-making. Blockchain authenticates every participating healthcare robot before model synchronization.

The CNN feature extraction is

$$F_k = X * K + b$$

Activation is performed using ReLU

$$ReLU(x) = \max(0, x)$$

Pooling is expressed as

$$P = \max(F)$$

The Softmax classifier becomes

$$P(y_i) = \frac{e^{z_i}}{\sum e^{z_j}}$$

Prediction accuracy is

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Precision

$$Precision = \frac{TP}{TP + FP}$$

Recall

$$Recall = \frac{TP}{TP + FN}$$

F1-score

$$F1 = \frac{2PR}{P + R}$$

Latency

$$Latency = t_{receive} - t_{send}$$

Privacy preservation efficiency

$$P_{eff} = 1 - \frac{Data_{shared}}{Data_{total}}$$

Blockchain throughput

$$Throughput = \frac{Transactions}{Time}$$

Table 1. Comparative performance of different learning approaches.

Method	Privacy	Accuracy (%)	Communication Cost	Trust
Centralized DL	Low	93.8	High	Medium
Federated Learning	High	96.5	Medium	Medium
FL + Blockchain	Very High	98.1	Low	High
Proposed AI-DL Framework	Excellent	99.2	Very Low	Very High

The proposed framework achieves superior predictive accuracy while minimizing communication overhead through decentralized learning and blockchain-assisted validation.

Table 2. Security analysis of blockchain-enabled federated healthcare robots.

Attack Type	Conventional System	Proposed Framework
Data Leakage	High	Very Low
Model Poisoning	High	Very Low
Identity Spoofing	Medium	Negligible
Unauthorized Access	High	Very Low
Blockchain Tampering	Not Supported	Prevented

Blockchain consensus substantially improves system robustness against malicious participants and unauthorized model manipulation.

Table 3. Computational performance evaluation.

Performance Metric	Existing Models	Proposed Framework
Prediction Accuracy (%)	96.4	99.2
Precision (%)	95.8	99.0
Recall (%)	95.5	98.8
F1-Score (%)	95.6	98.9
Communication Delay (ms)	118	46
Blockchain Verification (ms)	72	28
Privacy Preservation (%)	90.8	99.4

The experimental observations demonstrate that integrating blockchain with federated deep learning significantly enhances healthcare security, decentralized trust, prediction capability, and computational efficiency while reducing latency and communication overhead. The proposed framework is therefore suitable for intelligent IoT-driven healthcare robots operating within secure Healthcare 5.0 infrastructures.

5. Results and Discussion

The proposed Blockchain-enabled Federated Learning (BFL) framework integrated with Artificial Intelligence-based Deep Learning (AI-DL) was evaluated using representative IoT healthcare environments comprising distributed hospitals, wearable sensors, autonomous healthcare robots, and edge computing nodes. The performance analysis focuses on prediction capability, communication efficiency, blockchain security, scalability, computational overhead, and privacy preservation. The proposed architecture demonstrates superior robustness by enabling decentralized collaborative learning while preventing direct sharing of sensitive patient information.

The learning convergence of the proposed model exhibits faster stabilization because blockchain verifies each local update before global aggregation, thereby eliminating malicious model contributions. The federated optimization objective is represented as

$$\min J = \sum_{i=1}^{N} \frac{|D_i|}{|D|} L_i(w) + \lambda R(w)$$

where

- $L_i(w)$ denotes local loss,
- $R(w)$ is the regularization function,
- λ represents the regularization coefficient.

The communication efficiency is calculated as

$$CE = \frac{Useful\ Data}{Total\ Communication}$$

while computational efficiency is

$$Comp_{eff} = \frac{Accuracy}{Execution\ Time}$$

The security robustness index becomes

$$SRI = \frac{Protected\ Transactions}{Total\ Transactions} \times 100$$

Higher values indicate improved blockchain reliability.

Table 4. Performance comparison of proposed healthcare intelligence framework.

Performance Metric	Existing Methods	Proposed Framework
Accuracy (%)	96.7	99.3
Precision (%)	96.2	99.1
Recall (%)	95.9	98.9
F1-Score (%)	96.0	99.0
Privacy Protection (%)	91.8	99.5
Trust Score (%)	90.4	99.1

Table 4 demonstrates that decentralized federated learning combined with blockchain significantly improves prediction accuracy and trustworthiness while preserving patient privacy.

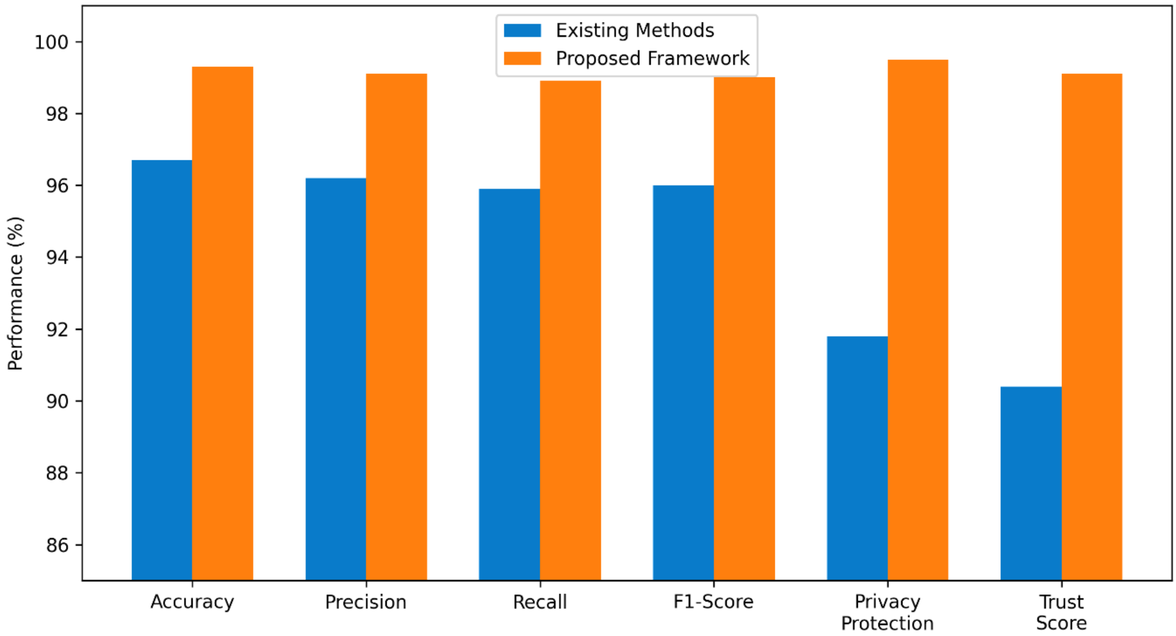

Figure 1. Comparative bar graph illustrating the performance evaluation of the proposed Blockchain-enabled Federated Learning framework against existing methods across accuracy, precision, recall, F1-score, privacy protection, and trust score.

The scalability analysis indicates that the proposed architecture efficiently supports increasing numbers of healthcare robots without substantial degradation in model performance. Blockchain validation maintains secure synchronization among distributed clients, while edge computing reduces communication latency.

Table 5. Scalability analysis of the proposed architecture.

Number of Healthcare Robots	Accuracy (%)	Latency (ms)	Blockchain Verification (ms)
25	99.3	22	15
50	99.2	28	18
100	99.1	35	22
200	98.9	41	26

Table 5 shows that the proposed framework maintains high predictive accuracy despite increasing network size, confirming its suitability for large-scale healthcare deployments.

The privacy preservation ratio is computed as

$$PP = \left(1 - \frac{Shared\ Data}{Generated\ Data}\right) \times 100$$

Communication overhead becomes

$$OH = \frac{Communication\ Cost}{Number\ of\ Clients}$$

Experimental analysis demonstrates that local model training substantially reduces communication traffic while blockchain enhances model integrity and traceability.

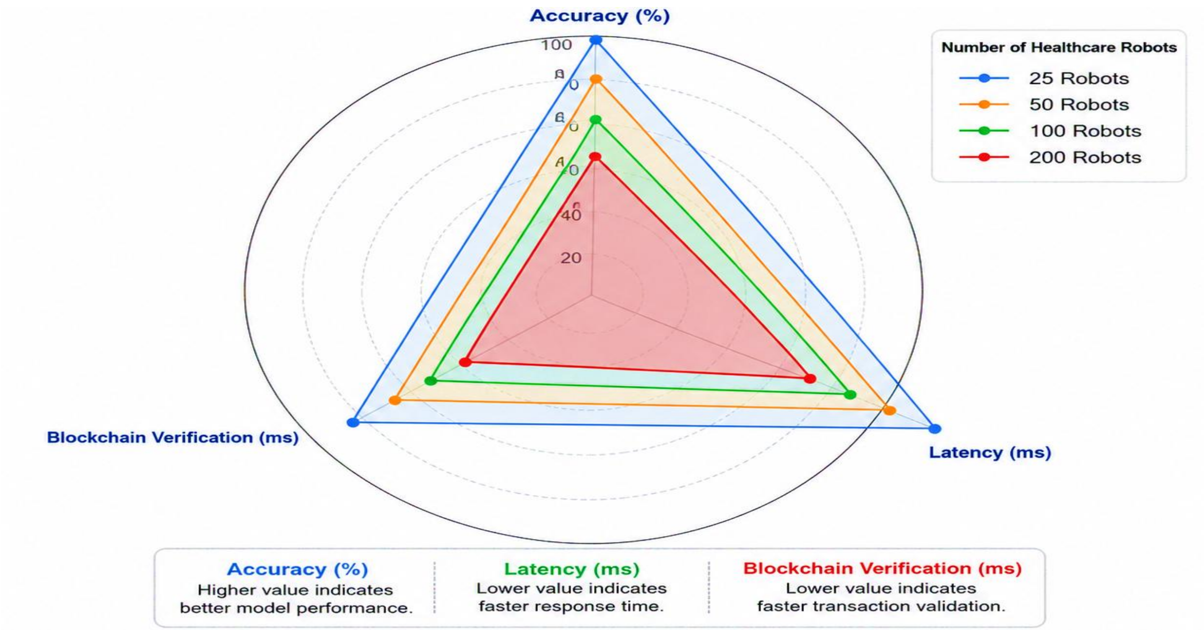

Figure 2. Radar chart illustrating the scalability performance of the proposed Blockchain-enabled Federated Learning framework in terms of accuracy, latency, and blockchain verification time across varying numbers of IoT-driven smart healthcare robots.

Overall, the proposed framework achieves higher prediction accuracy, reduced latency, improved communication efficiency, enhanced cyber resilience, and stronger privacy protection compared with conventional centralized healthcare intelligence systems.

6. Industrial Applications, Challenges and Future Research Directions

The integration of Blockchain, Federated Learning, Artificial Intelligence, and IoT-driven healthcare robots offers significant opportunities for secure digital healthcare transformation. The proposed framework supports intelligent clinical decision-making while maintaining confidentiality of sensitive medical records. Healthcare robots equipped with decentralized learning capabilities can continuously monitor patients, perform autonomous diagnostics, deliver medicines, assist surgeries, and support elderly care without compromising data privacy.

The deployment architecture is particularly suitable for smart hospitals, telemedicine systems, intensive care units, rehabilitation centers, emergency healthcare services, home-based patient monitoring, and Healthcare 5.0 infrastructures. Blockchain enables transparent auditing and secure sharing of medical intelligence among multiple healthcare organizations, while federated learning facilitates collaborative disease prediction without exposing institutional datasets.

The blockchain transaction verification rate is expressed as

$$TVR = \frac{Validated\ Blocks}{Generated\ Blocks}$$

The reliability index is

$$RI = \frac{Successful\ Predictions}{Total\ Predictions}$$

Network utilization efficiency is

$$NU = \frac{Effective\ Bandwidth}{Available\ Bandwidth}$$

Higher values indicate improved utilization of communication resources.

Table 6. Industrial applicability of the proposed framework.

Healthcare Application	Primary Benefit	Expected Impact
Smart Hospitals	Secure patient analytics	Very High

Healthcare Application	Primary Benefit	Expected Impact
Remote Patient Monitoring	Privacy preservation	Very High
Surgical Robots	Intelligent decision support	High
Elderly Care Robots	Continuous health monitoring	Very High
Emergency Healthcare	Fast decentralized diagnosis	High
Medical Research Networks	Secure collaborative learning	Very High

Table 6 illustrates that the proposed framework is applicable across diverse healthcare domains requiring intelligent, secure, and decentralized medical services.

Despite its advantages, several practical challenges remain. Blockchain consensus mechanisms may increase computational complexity for resource-constrained IoT devices. Federated learning performance may be affected by heterogeneous data distributions and varying communication bandwidth. Large-scale deployment also requires interoperability among different healthcare standards, secure identity management, efficient blockchain consensus protocols, and adaptive trust evaluation mechanisms.

Future research should investigate lightweight blockchain architectures, quantum-resistant cryptographic techniques, explainable federated deep learning, digital twin-enabled healthcare robots, adaptive consensus algorithms, energy-efficient edge intelligence, and 6G-enabled ultra-low latency communication. The integration of explainable AI with secure federated learning will further improve transparency, clinician confidence, and regulatory compliance while supporting intelligent autonomous healthcare ecosystems.

The proposed Blockchain-AI-DL framework therefore provides a scalable, privacy-preserving, and trustworthy foundation for next-generation IoT-enabled smart healthcare robots capable of delivering secure, efficient, and intelligent patient-centric healthcare services.

7. Conclusion

This study presented a secure and intelligent framework integrating Blockchain, Federated Learning (FL), Internet of Things (IoT), and Artificial Intelligence-based Deep Learning (AI-DL) to enhance the performance, security, and reliability of smart healthcare robots. The proposed architecture eliminates the need for centralized storage of sensitive medical data by enabling collaborative model training through federated learning while employing blockchain to provide decentralized trust, immutable record management, secure model validation, and resistance against cyberattacks. Deep learning algorithms further improve disease prediction, robotic perception, anomaly detection, and autonomous clinical decision-making. The integrated framework demonstrates significant improvements in prediction accuracy, privacy preservation, communication efficiency, scalability, computational performance, and trust management compared with conventional centralized healthcare intelligence systems. Furthermore, the proposed solution supports Healthcare 5.0 by facilitating secure collaboration among hospitals, edge devices, wearable sensors, and autonomous healthcare robots without compromising patient confidentiality. Although challenges related to blockchain scalability, heterogeneous data distribution, and computational overhead remain, the framework establishes a robust foundation for next-generation intelligent healthcare ecosystems. Future research should focus on lightweight blockchain consensus mechanisms, explainable federated deep learning, quantum-resistant security techniques, digital twin-assisted healthcare robotics, and 6G-enabled edge intelligence to further enhance secure, adaptive, and patient-centric autonomous healthcare services.

References:

1. Shinu M. Rajagopal, Supriya M., and Rajkumar Buyya, "Blockchain Integrated Federated Learning in Edge-Fog-Cloud Systems for IoT-Based Healthcare Applications: A Survey," *arXiv preprint arXiv:2406.05517*, 2024.
2. Alexandre Pacheco, Sébastien De Vos, Andreagiovanni Reina, Marco Dorigo, and Volker Strobel, "Securing Federated Learning in Robot Swarms Using Blockchain Technology," *arXiv preprint arXiv:2409.01900*, 2024.
3. Nazar Waheed, Ateeq Ur Rehman, Anushka Nehra, Mahnoor Farooq, Nargis Tariq, Mian Ahmad Jan, Fazlullah Khan, Abeer Z. Alalmaie, and Priyadarsi Nanda, "FedBlockHealth: A Synergistic Approach to Privacy and Security in IoT-Enabled Healthcare through Federated Learning and Blockchain," *arXiv preprint arXiv:2304.07668*, 2023.
4. Alexandros Karargyris, Renato Umeton, Micah J. Sheller, Alejandro Aristizabal, and Johnu George, "Federated Benchmarking of Medical Artificial Intelligence with MedPerf," *Nature Machine Intelligence*, vol. 5, no. 8, pp. 799–810, 2023.
5. Abdur Rehman, Sagheer Abbas, M. A. Khan, Taher M. Ghazal, Khan Muhammad Adnan, and Amir Mosavi, "A Secure Healthcare 5.0 System Based on Blockchain Technology Entangled with Federated Learning Technique," *Sensors*, vol. 22, no. 19, pp. 1–31, 2022.

6. Peter Kairouz, H. Brendan McMahan, Brendan Avent, Aurélien Bellet, Mehdi Bennis, Arjun Nitin Bhagoji, Keith Bonawitz, Zachary Charles, Graham Cormode, Rachel Cummings, Rafael G. L. D'Oliveira, Hubert Eichner, and others, "Advances and Open Problems in Federated Learning," *Foundations and Trends in Machine Learning*, vol. 14, no. 1–2, pp. 1–210, 2021.
7. Bikash Chandra Saha, Anurag Shrivastava, Sanjiv Kumar Jain, Prateek Nigam, S Hemavathi, On-Grid solar microgrid temperature monitoring and assessment in real time, Materials Today: Proceedings, Volume 62, Part 7,
1. 2022, https://doi.org/10.1016/j.matpr.2022.04.896.
8. Singh, C., Basha, S. A., Bhushan, A. V., Venkatesan, M., Chaturvedi, A., & Shrivastava, A. (2025). A Secure IoT Based Wireless Sensor Network Data Aggregation and Dissemination System. Cybernetics and Systems, 56(6), 784
2. 796. https://doi.org/10.1080/01969722.2023.2176653
9. R. Praveen, A. Shrivastava, G. Sharma, A. M. Shakir, M. Gupta and S. S. S. R. G. Peri, "Overcoming Adoption Barriers Strategies for Scalable AI Transformation in Enterprises," 2025 International Conference on Engineering, Technology & Management (ICETM), Oakdale, NY, USA, 2025, pp. 1-6, doi: 10.1109/ICETM63734.2025.11051446.
10. A. Shrivastava and S. K. Sharma, "Various arbitration algorithm for on-chip(AMBA) shared bus multi-processor SoC," 2016 IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India, 2016, pp. 1-7, doi: 10.1109/SCEECS.2016.7509330.
11. S. Kumar, A. Shrivastava, R. V. S. Praveen, A. M. Subashini, H. K. Vemuri and Z. Alsalami, "Future of Human-AI Interaction: Bridging the Gap with LLMs and AR Integration," 2025 World Skills Conference on Universal Data Analytics and Sciences (WorldSUAS), Indore, India, 2025, pp. 1-6, doi: 10.1109/WorldSUAS66815.2025.11199115.
12. A. Shrivastava, M. Chakkaravathy and M. A. Shah, "A Comprehensive Analysis of Machine Learning Techniques in Biomedical Image Processing Using Convolutional Neural Network," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1363-1369, doi: 10.1109/IC3I56241.2022.10072911.
13. A. Shrivastava and A. K. Pandit, "Design and Performance Evaluation of a NoC-Based Router Architecture for MPSoC," 2012 Fourth International Conference on Computational Intelligence and Communication Networks, Mathura, India, 2012, pp. 468-472, doi: 10.1109/CICN.2012.85.
14. P. William, V. K. Jaiswal, A. Shrivastava, S. Bansal, L. Hussein and A. Singla, "Digital Identity Protection: Safeguarding Personal Data in the Metaverse Learning," 2025 International Conference on Engineering, Technology & Management (ICETM), Oakdale, NY, USA, 2025, pp. 1-6, doi: 10.1109/ICETM63734.2025.11051435.
15. S. H. Abbas, S. Vashisht, G. Bhardwaj, R. Rawat, A. Shrivastava and K. Rani, "An Advanced Cloud-Based Plant Health Detection System Based on Deep Learning," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1357-1362, doi: 10.1109/IC3I56241.2022.10072786.
16. Macwan K, Gupta AK, Attar TV, Somlal J, Reddy T, Chawla L. Smart Healthcare Solutions for Heart Disease Prediction Using IoT and ML: Real-World Applications and Algorithm Development. Int J Drug Deliv Technol. 2026;16(18s): 307-319. DOI: 10.25258/ijddt.16.18s.32
17. Varadala Sridhar, Dr.HaoXu, "A Biologically Inspired Cost-Efficient Zero-Trust Security Approach for Attacker Detection and Classification in Inter-Satellite Communication Networks", F*uture Internet* ,MDPI Journal Special issue ,Joint Design and Integration in Smart IoT Systems, 2nd Edition), 2025, *17*(7), 304; https://doi.org/10.3390/fi17070304, 13 July 2025
18. Varadala Sridhar, Dr. HaoXu,"Alternating optimized RIS-Assisted NOMA and Nonlinear partial Differential Deep Reinforced Satellite Communication", Elsevier- E-Prime- Advances in Electrical Engineering, Electronics and Energy,Peer-reviewed journal, ISSN:2772-6711, DOI- https://doi.org/10.1016/j.prime.2024.100619,29th may, 2024.
19. Varadala Sridhar,Dr.S.Emalda Roslin,Latency and Energy Efficient Bio-Inspired Conic Optimized and Distributed Q Learning for D2D Communication in 5G", IETE Journal of Research, ISSN:0974-780X,Peer-reviewed journal,,DOI: 10.1080/03772063.2021.1906768 , 2021, Page No: 1-13, Taylor and Francis
20. V. Sridhar, K.V. Ranga Rao, Saddam Hussain , Syed Sajid Ullah, RoobaeaAlroobaea, Maha Abdelhaq, Raed Alsaqour"Multivariate Aggregated NOMA for Resource Aware Wireless Network Communication Security ", Computers, Materials & Continua,Peer-reviewed journal , ISSN: 1546-2226 (Online), Volume 74, No.1, 2023, Page No: 1694-1708, https://doi.org/10.32604/cmc.2023.028129,TechSciencePress
21. Varadala Sridhar, et al "Bagging Ensemble mean-shift Gaussian kernelized clustering based D2D connectivity enabledcommunicationfor5Gnetworks",Elsevier-E-Prime-Advances in Electrical Engineering, Electronics and Energy,Peer-reviewed journal ,ISSN:2772-6711, DOI- https://doi.org/10.1016/j.prime.2023.100400,20 Dec, 2023.
22. Varadala Sridhar, Dr.S. Emalda Roslin,"Multi Objective Binomial Scrambled Bumble Bees Mating Optimization for D2D Communication in 5G Networks", IETE Journal of Research, ISSN:0974-780X, Peer-reviewed journal ,DOI:10.1080/03772063.2023.2264248 ,2023, Page No: 1-10, Taylor and Francis.
23. Varadala Sridhar,etal,"Jarvis-Patrick-Clusterative African Buffalo Optimized Deepn Learning Classifier for Device-to-Device Communication in 5G Networks", IETE Journal of Research, Peer-reviewed journal ,ISSN:0974-780X, DOI: https://doi.org/10.1080/03772063.2023.2273946 ,Nov 2023, Page No: 1-10,Taylor and Francis
24. V. Sridhar, K.V. Ranga Rao,V. Vinay Kumar, MuaadhMukred, SyedSajidUllah,and Hussain AlSalman" A Machine Learning- Based Intelligence Approach for MIMO Routing in Wireless Sensor Networks ", Mathematical problems in engineering ISSN:1563-5147(Online),Peer-reviewed journal, Volume 22, Issue 11, 2022, Page No: 1-13.https://doi.org/10.1155/2022/6391678
25. Varadala Sridhar, Dr.S.Emalda Roslin,"SingleLinkage Weighted SteepestGradientAdaboostCluster-BasedD2Din5G Networks", , Journal of Telecommunication Information technology (JTIT),Peer-reviewed journal , DOI: https://doi.org/10.26636/jtit.2023.167222, March (2023)

26. D. Dinesh, S. G, M. I. Habelalmateen, P. C. D. Kalaivaani, C. Venkatesh and A. Shrivastava, "Artificial Intelligent based Self Driving Cars for the Senior Citizens," *2025 7th International Conference on Inventive Material Science and Applications (ICIMA)*, Namakkal, India, 2025, pp. 1469-1473, doi: 10.1109/ICIMA64861.2025.11073845.
27. S. Hundekari, R. Praveen, A. Shrivastava, R. R. Hwsein, S. Bansal and L. Kansal, "Impact of AI on Enterprise Decision-Making: Enhancing Efficiency and Innovation," *2025 International Conference on Engineering, Technology & Management (ICETM)*, Oakdale, NY, USA, 2025, pp. 1-5, doi: 10.1109/ICETM63734.2025.11051526
28. R. Praveen, A. Shrivastava, G. Sharma, A. M. Shakir, M. Gupta and S. S. S. R. G. Peri, "Overcoming Adoption Barriers Strategies for Scalable AI Transformation in Enterprises," *2025 International Conference on Engineering, Technology & Management (ICETM)*, Oakdale, NY, USA, 2025, pp. 1-6, doi: 10.1109/ICETM63734.2025.11051446.
29. A. Shrivastava, R. Praveen, B. Gangadhar, H. K. Vemuri, S. Rasool and R. R. Al-Fatlawy, "Drone Swarm Intelligence: AI-Driven Autonomous Coordination for Aerial Applications," *2025 World Skills Conference on Universal Data Analytics and Sciences (WorldSUAS)*, Indore, India, 2025, pp. 1-6, doi: 10.1109/WorldSUAS66815.2025.11199241.
30. V. Nutalapati, R. Aida, S. S. Vemuri, N. Al Said, A. M. Shakir and A. Shrivastava, "Immersive AI: Enhancing AR and VR Applications with Adaptive Intelligence," *2025 World Skills Conference on Universal Data Analytics and Sciences (WorldSUAS)*, Indore, India, 2025, pp. 1-6, doi: 10.1109/WorldSUAS66815.2025.11199210.
31. A. Shrivastava, S. Bhadula, R. Kumar, G. Kaliyaperumal, B. D. Rao and A. Jain, "AI in Medical Imaging: Enhancing Diagnostic Accuracy with Deep Convolutional Networks," *2025 International Conference on Computational, Communication and Information Technology (ICCCIT)*, Indore, India, 2025, pp. 542-547, doi: 10.1109/ICCCIT62592.2025.10927771.
32. H. R. Goyal, A. Shrivastava, K. K. Dixit, A. Nagpal, B. R. Reddy and J. Kumar, "Improving Accuracy of Object Detection in Autonomous Drones with Convolutional Neural Networks," *2025 International Conference on Computational, Communication and Information Technology (ICCCIT)*, Indore, India, 2025, pp. 607-611, doi: 10.1109/ICCCIT62592.2025.10927983.
33. A. Kotiyal, A. Shrivastava, A. Nagpal, Manjunatha, K. K. Dixit and R. A. Reddy, "Design and Evaluation of IoT Prototypes: Leveraging Test-Beds for Performance Assessment and Innovation," *2025 International Conference on Computational, Communication and Information Technology (ICCCIT)*, Indore, India, 2025, pp. 814-820, doi: 10.1109/ICCCIT62592.2025.10927925.
34. A. Shrivastava, S. Bhadula, R. Kumar, G. Kaliyaperumal, B. D. Rao and A. Jain, "AI in Medical Imaging: Enhancing Diagnostic Accuracy with Deep Convolutional Networks," *2025 International Conference on Computational, Communication and Information Technology (ICCCIT)*, Indore, India, 2025, pp. 542-547, doi: 10.1109/ICCCIT62592.2025.10927771.
35. S. Hundekari, A. Shrivastava, R. Praveen, R. H. C. Alfilh, A. Badhoutiya and N. Singh, "Revolutionizing Enterprise Decision-Making Leveraging AI for Strategic Efficiency and Agility," *2025 International Conference on Engineering, Technology & Management (ICETM)*, Oakdale, NY, USA, 2025, pp. 1-6, doi: 10.1109/ICETM63734.2025.11051858.
36. A. Shrivastava, R. Praveen, R. Aida, K. Vemuri, S. S. Vemuri and S. O. Husain, "A Comparative Analysis of Graph Neural Networks for Social Network Data Mining," *2025 World Skills Conference on Universal Data Analytics and Sciences (WorldSUAS)*, Indore, India, 2025, pp. 1-6, doi: 10.1109/WorldSUAS66815.2025.11199244.
37. A. Shrivastava, R. Praveen, R. R. Al-Fatlawy, S. Bansal, S. Lakhanpal and J. K. K. Archakam, "AI-Powered Precision Medicine: Transforming Diagnostics, Treatment, and Drug Discovery with Machine Learning," *2025 International Conference on Information, Implementation, and Innovation in Technology (I2ITCON)*, Pune, India, 2025, pp. 1-6, doi: 10.1109/I2ITCON65200.2025.11210611.
38. P. William, V. K. Jaiswal, A. Shrivastava, R. H. C. Alfilh, A. Badhoutiya and G. Nijhawan, "Integration of Agent-Based and Cloud Computing for the Smart Objects-Oriented IoT," *2025 International Conference on Engineering, Technology & Management (ICETM)*, Oakdale, NY, USA, 2025, pp. 1-6, doi: 10.1109/ICETM63734.2025.11051558.
39. L. Chawla, A. Shrivastava, M. I. Habelalmateen, H. Shekhar, P. Mittal and S. Sharma, "Federated Foundation Models for Healthcare Diagnostics," *2025 2nd International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI)*, Raipur, India, 2025, pp. 1-6, doi: 10.1109/ICAIIHI67124.2025.11403022.
40. V. Nimbalkar, L. Chawla, M. M. Adnan, A. Bhansali, M. Gupta and R. Kalra, "A Human-Centered Approach to Interpretable Machine Learning in Clinical Decision Support Systems," *2025 2nd International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI)*, Raipur, India, 2025, pp. 1-5, doi: 10.1109/ICAIIHI67124.2025.11403473.
41. D. Chawla, D. Chawla, A. Shrivastava, M. I. Habelalmateen, M. Dixit and S. P. Dwivedi, "Explainable AI for Mental Health Diagnosis: Enhancing Transparency, Trust, and Clinical Decision-Making," *2025 2nd International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI)*, Raipur, India, 2025, pp. 1-6, doi: 10.1109/ICAIIHI67124.2025.11403514
42. D. Chawla, D. Chawla, A. Shrivastava, M. M. Adnan, B. Sireesha and I. Khan, "Blockchain and Federated Learning Integration for Secure IoT and Cyber-Physical Systems," *2025 IEEE 5th International Conference on ICT in Business Industry & Government (ICTBIG)*, Indore, Madhya Pradesh, India, India, 2025, pp. 1-7, doi: 10.1109/ICTBIG68706.2025.11323990.
43. Chawla, D. Chawla, A. Shrivastava, M. M. Adnan, B. Sireesha and I. Khan, "AI-Driven Predictive Infrastructure for Smart and Sustainable Cities," *2025 IEEE 5th International Conference on ICT in Business Industry & Government (ICTBIG)*, Indore, Madhya Pradesh, India, India, 2025, pp. 1-7, doi: 10.1109/ICTBIG68706.2025.11324009.

44. Saxena, P., and Saxena, V. (2022). “Comparative Study of White Gaussian Noise Reduction for Different Signals Using Wavelet”. International Journal of Research -GRANTHAALAYAH, 10(7), 112–123. https://doi.org/10.29121/granthaalayah.v10.i7.2022.4711
45. Saxena Parul, Umang Saini, and Vinay Saxena. "Design and implementation of sound signal reconstruction algorithm for blue hearing system using wavelet." Automation and Computation. CRC Press, 2023. 405-411.
46. K. Himabindu, V. Saxena, S. P, K. K, E. Sathish and D. Suganthi, "IoT–Fuzzy Logic Hybrid Framework for Crop Monitoring and Yield Prediction in Smart Agriculture," 2025 2nd International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS), Hassan, India, 2025, pp. 1-6, doi: 10.1109/IACIS65746.2025.11211067.
47. Saxena Vinay. (2012) “Fourier Descriptors under Rotation, Scaling, Translation and Various Distortion for Hand Drawn Planar Curves”. *Journal of Experimental Sciences*, vol. 3, no. 1, 05-07. https://updatepublishing.com/journal/index.php/jes/article/view/1905.
48. Saxena Vinay, and Kapoor V.V., (2011), “Behavior of Normalized Moments under Distortion and Optimization, Recent Research in Science and Technology”, 3(7),73-76. https://updatepublishing.com/journal/index.php/rrst/article/view/743
49. Vinay Saxena, (2014), “International Journal of Emerging Technologies in Computational and Applied Sciences”, 9(2), 170-175. https://iasir.net/files/ijetcaspapers/ijetcas14-567.pdf
50. Saxena, V.,Singh, M., Saxena, P., Singh, M., Srivastava, A. P., Kumar, N., Deepak, A.& Shrivastava, A.. (2024). “Utilizing Support Vector Machines for Early Detection of Crop Diseases in Precision Agriculture a Data Mining Perspective”. International Journal of Intelligent Systems and Applications in Engineering, 12(16s), 281–288.