International Journal of Basic and Applied Sciences, 14 (1) (2025) 246-250

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS

https://doi.org/10.14419/n1npsj75

Research paper

A Federated Learning and Blockchain Framework for IoMT-Driven Healthcare 5.0

Denis R. [1], N. Venkateswaran [2], S. Gangadharan [3], M. Shunmugasundaram [4], Guduri Chitanya [5], Girija M. S. [6], V. V. Satyanarayana Tallapragada [7], R. G. Vidhya [8]*

[1] Department of Computer Science, Mount Carmel College Autonomous, Bengaluru, Karnataka, India.
[2] Department of Master of Business Administration, Panimalar Engineering College, Chennai, Tamil Nadu, India.
[3] Department of Management Studies, St. Joseph's College of Engineering, Chennai, Tamil Nadu, India.
[4] Department of Management Studies, St. Joseph's College of Engineering, Chennai, Tamil Nadu, India.
[5] Department of English, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India.
[6] Department of Computer Science and Design, R.M.K Engineering College, Kavaraipettai, Tamil Nadu, India.
[7] Department of ECE, School of Engineering, Mohan Babu University, Tirupati, Andhra Pradesh, India.
[8] Department of ECE, HKBK College of Engineering, Bangalore, India.*
**Corresponding author E-mail: s61537104@gmail.com*

Received: March 21, 2025, Accepted April 30, 2025, Published: May 11, 2025

Abstract

This paper presents an innovative framework integrating federated learning, blockchain, and the Internet of Medical Things (IoMT) to revolutionize healthcare systems in the context of Healthcare 5.0. By harnessing advanced sensors and leveraging 5G technology, the framework enables continuous, real-time data collection and intelligent analysis, facilitating highly personalized and timely medical interventions. Federated learning enables decentralized model training across edge devices, preserving data privacy and enhancing security. Simultaneously, blockchain ensures the integrity and transparency of healthcare records through a decentralized and tamper-proof ledger. The synergy of these technologies fosters secure and efficient communication across a network of interconnected medical devices. This framework significantly enhances healthcare delivery by promoting proactive, patient-focused, and adaptive care models. Additionally, IoMT expands the capabilities of medical equipment by enabling remote monitoring, automated data transmission, and comprehensive patient oversight. As the vision of Healthcare 5.0 progresses, embracing such cutting-edge technological solutions is vital for improving patient outcomes, streamlining operations, and accelerating medical innovation. Through the combined power of federated learning, blockchain, and IoMT, the healthcare sector stands on the brink of a transformative shift toward secure, intelligent, and personalized care.

Keywords: *Internet of Medical Things; Healthcare 5.0; Secure Data Exchange; Federated Learning; Blockchain Technology.*

1. Introduction

The healthcare industry is undergoing a transformative shift driven by cutting-edge digital technologies, marking the emergence of healthcare 5.0 [1], [2]. This next-generation healthcare model emphasizes precision, personalization, and patient-centric care through the integration of technologies such as federated learning, blockchain, the Internet of Medical Things (IoMT), and advanced medical sensors [3], [4]. Federated learning facilitates the decentralized training of machine learning models across various edge devices, ensuring that sensitive patient data remains localized and secure [5], [6]. Blockchain introduces a tamper-resistant, decentralized infrastructure that guarantees transparency and trust in healthcare data exchange and management [7], [8]. IoMT, composed of a network of smart medical devices and wearable sensors, enables the seamless collection and processing of health data in real time [9], [10]. The evolution of sensor technology and high-speed connectivity has empowered these devices to continuously monitor patient health, providing critical insights that support timely and personalized interventions [11], [12]. Together, these technologies are reshaping how care is delivered, making it more responsive, secure, and efficient [13], [14]. Fig. 1 illustrates a conceptual architecture of blockchain implementation within this healthcare framework.

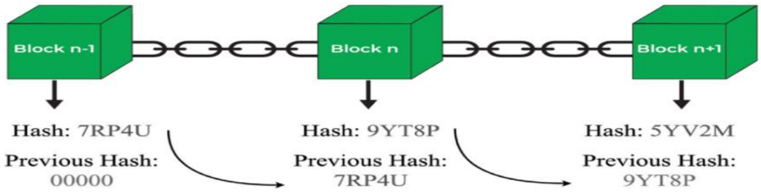


Fig. 1: Blockchain Architecture.

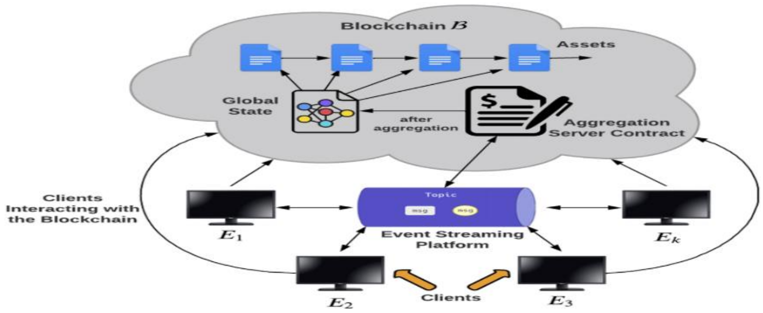


Fig. 2: Federated Learning.

2. Proposed methodology

The proposed framework for a next-generation smart healthcare system integrates several advanced technologies—including blockchain, federated learning, and the Real-Time Deep Extreme Learning Machine (RTS-DELM)—to deliver secure, intelligent, and privacy-preserving healthcare services. This methodology has been designed with a strong emphasis on interoperability, scalability, and robustness, aiming to fulfil the core objectives of healthcare 5.0 [15], [16]. The foundation of the secure data exchange mechanism within the system begins with the integration of blockchain technology [17], [18]. The selection of an appropriate blockchain platform is critical and involves evaluating features such as transaction throughput, latency, consensus protocol (e.g., Proof of Stake, Practical Byzantine Fault Tolerance), data privacy capabilities, and cost-efficiency [19], [20]. Once the platform is finalized, a distributed network architecture is established. This includes defining key entities such as peer nodes, orderers, and communication channels [21], [22]. Nodes represent different healthcare institutions or IoMT devices, and channels ensure privacy by isolating transactions among authorized participants [23], [24]. To automate essential healthcare processes, smart contracts (or chain codes) are developed and deployed on the blockchain network. These smart contracts govern access permissions, patient data sharing protocols, billing and insurance verification processes, and consent management [25], [26]. All transactions are cryptographically secured using SHA-256 or similar hashing algorithms, and public-key infrastructure (PKI) is used for identity verification and authentication of users [27], [28]. Blockchain's immutable ledger ensures that all health-related data exchanges are transparent and tamper-proof. Access control is enforced through Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC) models, while data privacy is enhanced using zero-knowledge proofs and secure multiparty computation techniques [29], [30]. Integration with existing healthcare systems (e.g., Electronic Health Records or hospital information systems) is achieved via standardized APIs and middleware services. Parallel to blockchain integration, the RTS-DELM module is implemented to process high-velocity healthcare data in real-time [31], [32]. RTS-DELM is a computationally optimized deep learning framework designed for rapid data analysis with minimal latency. This makes it particularly suitable for edge-level decision-making in IoMT ecosystems [33], [34]. The model architecture selection is guided by real-time constraints, such as minimal model complexity, high convergence speed, and scalability. Medical data is continuously collected from diverse sources such as wearable health monitors, body sensor networks (BSNs), and IoT-enabled diagnostic equipment [35,36]. This streaming data is fed into the RTS-DELM model for pre-processing, feature extraction, and classification. Hardware accelerators such as GPUs or FPGAs are employed to boost computational efficiency [37]. The model is trained using federated learning, which allows multiple institutions or devices to collaboratively learn a shared prediction model without exposing local data [38]. This decentralized training preserves data locality and complies with regulations such as HIPAA and GDPR. Differential privacy techniques are applied to ensure that individual patient identities cannot be inferred from the trained model [39,40]. To further strengthen the security architecture, an Intrusion Detection System (IDS) is embedded within the network layer of the system [41]. The IDS continuously monitors system and network logs, inspecting incoming and outgoing data packets to detect anomalies or known attack signatures [42]. Using machine learning-based anomaly detection, the IDS identifies patterns linked to unauthorized access attempts, denial-of-service (DoS) attacks, data breaches, and other threats [43], [44]. The NSL-KDD dataset is used to train and test the IDS component. It includes labelled data capturing various forms of legitimate and malicious network activity [45]. The dataset is preprocessed to normalize attributes, remove noise, and select relevant features for model training [46]. Each network connection is categorized into one of several attack classes (e.g., R2L, U2R, Probe, DoS), and the system learns to differentiate between normal and malicious behaviour in real-time. Fig. 2 shows the Federated Learning

Parkinson's Disease Dataset: This dataset contains comprehensive clinical information, including demographic data, medical histories, diagnostic scores, and symptom progression indicators. It is used for training and evaluating the RTS-DELM model’s ability to predict and monitor neurological disorders.

NSL-KDD Dataset: A benchmark dataset widely adopted in cybersecurity research for evaluating intrusion detection systems. It includes a variety of network traffic features (e.g., IP addresses, protocol types, port numbers) and classifies each instance as normal or under attack [47]. The datasets are divided using a stratified sampling approach—70% of the data is allocated for training, and the remaining 30% is split between validation and testing sets [48]. The model's performance is assessed using a diverse set of evaluation metrics, including Accuracy, Sensitivity (Recall), Specificity, Precision (PPV) –Negative Predictive Value (NPV), True Positive Rate (TPR), and True Negative Rate (TNR), Miss Rate. By harmoniously combining federated learning, blockchain, RTS-DELM, and IDS functionalities, the proposed framework achieves a robust, intelligent healthcare infrastructure. This comprehensive approach aligns with the principles of healthcare 5.0—delivering intelligent, data-driven, secure, and patient-centric medical care that adapts to the rapidly evolving digital health landscape.

Table 1: Metrics Insights to the Performance of the RTS-DELM-Based System

Client	Accuracy	Sensitivity	Specificity	Negative Predictive Value	False Positive Rate	False Discovery Rate	False Negative Rate
1	0.94	0.88	0.88	0.96	0.04	0.11	0.12
2	0.92	0.85	0.85	0.94	0.06	0.15	0.15
3	0.96	0.92	0.92	0.97	0.03	0.08	0.19

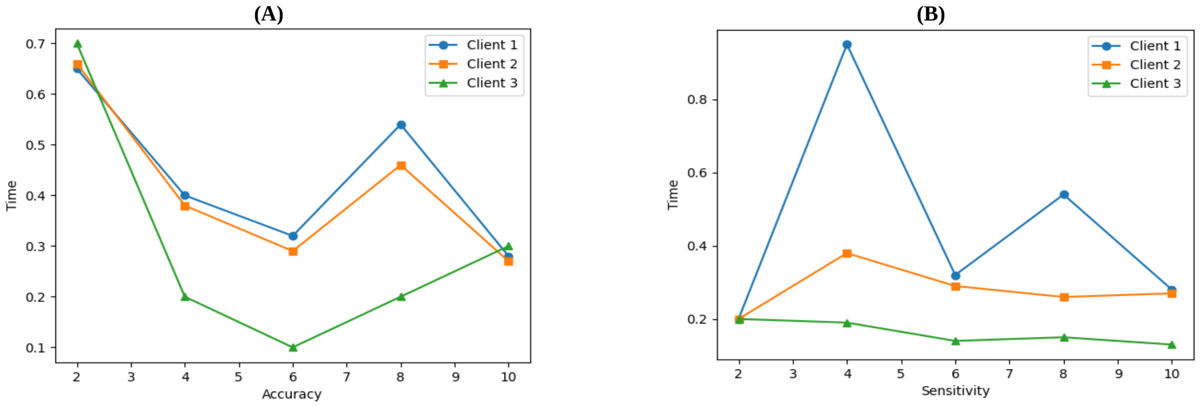
Table 2: Metrics Insights to the Performance of Intrusion Detection

Client	Accuracy	Sensitivity	Specificity	Negative Predictive Value	False Positive Rate	False Discovery Rate	False Negative Rate
1	93.75	98.25	82.61	95.25	17. 39	6.67	1.75
2	94.72	98.95	84.07	96.94	15.93	6	1.05
3	96.10	97.50	90.20	95.80	9.80	7.50	2.50

3. Results and discussions

This section presents the evaluation of the proposed RTS-DELM-based federated learning system deployed across three client environments. The performance is analysed based on multiple metrics, including accuracy, sensitivity, specificity, false positive rate (FPR), false discovery rate (FDR), false negative rate (FNR), and negative predictive value (NPV). The outcomes provide a comprehensive view of the system's efficacy in both health condition prediction and intrusion detection tasks. Tables 1 and 2 summarize the quantitative results, while Fig. 3 offers a visual comparison of key performance indicators. The performance of the RTS-DELM model on healthcare data is evaluated independently for each client. The model exhibits varying degrees of effectiveness, shaped by differences in local data distributions and federated training dynamics. Client 1 achieves an accuracy of 94%, indicating strong overall performance. It demonstrates sensitivity and specificity values of 88%, reflecting a balanced ability to correctly identify both positive and negative cases. A low false positive rate of 4% and a high NPV of 96% further underline the model’s strength in correctly ruling out non-critical instances. These metrics collectively suggest that Client 1 effectively minimizes false alarms while maintaining reliability in its diagnostic predictions. Client 2 records a slightly lower accuracy of 92%, with both sensitivity and specificity at 85%. While still robust, this balanced performance is accompanied by a false positive rate of 6% and a false discovery rate of 15%, indicating a modestly higher incidence of incorrect alerts compared to Client 1. Nonetheless, the model maintains a strong NPV, ensuring dependable identification of negative outcomes. Client 3 emerges as the top performer, with the highest accuracy at 96%, and superior sensitivity and specificity, both at 92%. These results suggest an optimal balance between correctly identifying diseased and non-diseased cases. However, a false negative rate of 19% raises concerns about missed positive cases, which may be attributed to localized data imbalances or edge-case variability in input features. These comparative outcomes, as presented in Table 1, provide critical insight into how the RTS-DELM model performs under different real-world client scenarios in health prediction tasks. In the context of cybersecurity, the RTS-DELM model was assessed for its capacity to detect intrusions within the system network using the NSL-KDD dataset. Each client was evaluated independently to reflect variations in traffic patterns and attack profiles. Client 1 achieves an accuracy of 93.75%, with an impressive sensitivity of 98.25%, indicating high effectiveness in detecting actual threats. However, a moderate specificity of 82.61% and a relatively high false positive rate of 17.39% suggest susceptibility to generating false alerts, which may lead to alert fatigue or unnecessary defensive actions. Client 2 slightly surpasses Client 1 in overall performance, achieving an accuracy of 94.72%. It boasts the highest sensitivity among all clients at 98.95%, making it highly reliable for threat detection. Furthermore, with a specificity of 84.07% and a lower false positive rate of 15.93%, it demonstrates a more favourable trade-off between detection and false alarms. The false discovery rate of just 6% further strengthens its operational credibility. Client 3, once again, stands out with the highest accuracy at 96.10% and a superior specificity of 90.20%, indicating the model’s excellence in identifying benign traffic and minimizing false positives (FPR = 9.80%). Although its sensitivity is slightly lower at 97.50%, the trade-off is justified by its reliability in discriminating normal from malicious behaviour. All clients demonstrate NPV values above 95%, ensuring dependable identification of non-threat events. Table 2 summarizes these metrics, while Figure 3 visually represents the comparative client performance. The results affirm that the model retains high generalizability and accuracy across varying network environments, with Client 3 presenting the most favourable balance of detection and reliability.

The overall results validate the efficacy of the RTS-DELM-based federated architecture for both clinical and security use cases. The federated learning approach enables clients to benefit from collective learning without compromising local data privacy, while the blockchain integration ensures secure and auditable data exchange. In healthcare monitoring, the model proves adept at early disease detection and risk assessment, although further enhancements in reducing false negatives (especially in Client 3) may improve patient safety in critical scenarios. In intrusion detection, the system exhibits excellent sensitivity and predictive performance, with manageable false positive rates. The deployment of IDS within the federated framework ensures a proactive cybersecurity shield without centralizing sensitive logs or compromising data integrity. The disparity in performance across clients highlights the importance of data quality, feature diversity, and localized training dynamics. Adaptive learning rate strategies and personalized federated updates could further enhance model consistency across heterogeneous environments.



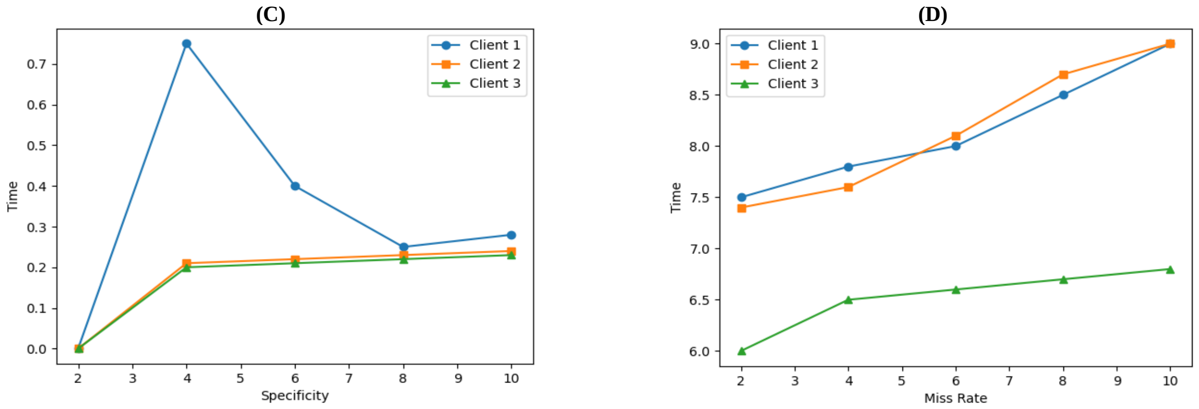


Fig. 3: Performance Metrics of Different Clients.

4. Conclusion

This study presents a comprehensive evaluation of a secure Healthcare 5.0 system built upon the Real-Time Deep Extreme Learning Machine (RTS-DELM) framework, integrated with federated learning and blockchain technologies. The results underscore the robustness and adaptability of the proposed approach in effectively addressing dual objectives: proactive healthcare monitoring and real-time intrusion detection across distributed client environments. Through rigorous experimentation using heterogeneous datasets—including clinical data for Parkinson's disease prediction and the NSL-KDD dataset for network intrusion detection—the system demonstrated consistently high performance. Metrics such as accuracy, sensitivity, specificity, and negative predictive value affirm the model's reliability in detecting both health-related anomalies and malicious network behaviours. While performance varied slightly across clients due to differing data distributions and system contexts, the system maintained overall integrity, exhibiting low false detection rates and high predictive precision. These findings highlight the critical importance of client-specific customization in federated learning-based systems, particularly within complex and sensitive domains such as healthcare. Moreover, the integration of blockchain enhances data security, transparency, and integrity, an essential feature for maintaining trust and compliance in digital health ecosystems. Importantly, this research demonstrates the feasibility of deploying intelligent, privacy-preserving AI solutions in real-world healthcare infrastructures without compromising patient confidentiality or data sovereignty. The RTS-DELM-based architecture not only enables real-time, decentralized decision-making but also aligns with the emerging demands of the industry 4.0 and Healthcare 5.0 paradigms. Moving forward, future work should focus on the continual refinement of the RTS-DELM model to further improve its adaptability, scalability, and resilience against evolving cybersecurity threats. Exploration into adversarial robustness, personalized federated learning, and adaptive consensus protocols will be essential to strengthen the system's performance in increasingly dynamic and heterogeneous environments. In summary, the proposed system represents a significant step toward building a secure, intelligent, and decentralized healthcare infrastructure capable of withstanding modern cyber challenges while promoting proactive, patient-centered care in the digital age.

References

[1] Aggarwal S, Gupta R, Sharma P, Verma M, Patel K." Exploring Blockchain Technology in Healthcare: Integrating Transactions, Home Healthcare, and Investment Distribution". Journal of Healthcare Engineering. 2019.

[2] Andoni M, Robu V, Flynn D, Abram S, Geach D. "Blockchain Applications in Peer-to-Peer Resource Sharing Networks: A Comprehensive Survey". IEEE Access. 2018; 6:10798-10825.

[3] Li G, Wang X, Zhou Y, Zhang H, Yang J. "Blockchain-Based User-Centric Communication Security Framework for IoT in Smart Home". IEEE Transactions on Computational Social Systems. 2020; 7(4):1063-1074.

[4] T. Al-Shehari, M. Kadrie, T. Alfakih, H. Alsalman, T. Kuntavai, et al., "Blockchain with secure data transactions and energy trading model over the internet of electric vehicles," Sci. Rep., vol. 14, no. 1, p. 19208, Jan. 2024, https://doi.org/10.1038/s41598-024-69542-w.

[5] R. Vidhya, D. Banavath, S. Kayalvili, S. M. Naidu, et al., "Alzheimer's disease detection using residual neural network with LSTM hybrid deep learning models," J. Intell. Fuzzy Syst., vol. 45, no. 6, pp. 12095–12109, 2023. https://doi.org/10.3233/JIFS-235059.

[6] P. Selvam, N. Krishnamoorthy, S. P. Kumar, K. Lokeshwaran, M. Lokesh, et al., "Internet of Things Integrated Deep Learning Algorithms Monitoring and Predicting Abnormalities in Agriculture Land," Internet Technol. Lett., Nov. 2024, https://doi.org/10.1002/itl2.607.

[7] K. Maithili, A. Kumar, D. Nagaraju, D. Anuradha, S. Kumar, et al., "DKCNN: Improving deep kernel convolutional neural network-based covid-19 identification from CT images of the chest," J. X-ray Sci. Technol., vol. 32, no. 4, pp. 913–930, 2024. https://doi.org/10.3233/XST-230424.

[8] K. Mannanuddin, V. R. Vimal, A. Srinivas, S. D. U. Mageswari, G. Mahendran, et al., "Enhancing medical image analysis: A fusion of fully connected neural network classifier with CNN-VIT for improved retinal disease detection," J. Intell. Fuzzy Syst., vol. 45, no. 6, pp. 12313–12328, 2023. https://doi.org/10.3233/JIFS-235055.

[9] T. A. Mohanaprakash, M. Kulandaivel, S. Rosaline, P. N. Reddy, S. S. N. Bhukya, et al., "Detection of Brain Cancer through Enhanced Particle Swarm Optimization in Artificial Intelligence Approach," J. Adv. Res. Appl. Sci. Eng. Technol., vol. 33, no. 3, pp. 174–186, 2023. https://doi.org/10.3233/JIFS-235055.

[10] Wange N. K., Khan I., Pinnamaneni R., Cheekati H., Prasad J., et al., "β-amyloid deposition-based research on neurodegenerative disease and their relationship in elucidate the clear molecular mechanism," Multidisciplinary Science Journal, vol. 6, no. 4, pp. 2024045–2024045, 2024. https://doi.org/10.31893/multiscience.2024045.

[11] Anitha C., Tellur A., Rao K. B. V. B., Kumbhar V., Gopi T., et al., "Enhancing Cyber-Physical Systems Dependability through Integrated CPS-IoT Monitoring," International Research Journal of Multidisciplinary Scope, vol. 5, no. 2, pp. 706–713, 2024. https://doi.org/10.47857/irjms.2024.v05i02.0620.

[12] Balasubramani R., Dhandapani S., Sri Harsha S., Mohammed Rahim N., Ashwin N., et al., "Recent Advancement in Prediction and Analyzation of Brain Tumour using the Artificial Intelligence Method," Journal of Advanced Research in Applied Sciences and Engineering Technology, vol. 33, no. 2, pp. 138–150, 2023. https://doi.org/10.37934/araset.33.2.138150.

[13] Chaturvedi A., Balasankar V., Shrimali M., Sandeep K. V., et al., "Internet of Things Driven Automated Production Systems using Machine Learning," International Research Journal of Multidisciplinary Scope, vol. 5, no. 3, pp. 642–651, 2024. https://doi.org/10.37934/araset.33.2.138150.

[14] Saravanakumar R., Arularasan A. N., Harekal D., Kumar R. P., Kaliyamoorthi P., et al., “Advancing Smart Cyber Physical System with Self-Adaptive Software,” International Research Journal of Multidisciplinary Scope, vol. 5, no. 3, pp. 571–582, 2024. https://doi.org/10.47857/irjms.2024.v05i03.01013.

[15] Vidhya R. G., Surendiran J., Saritha G., “Machine Learning Based Approach to Predict the Position of Robot and its Application,” Proc. Int. Conf. on Computer Power and Communications, pp. 506–511, 2022. https://doi.org/10.1109/ICCPC55978.2022.10072031.

[16] Sivanagireddy K., Yerram S., Kowsalya S. S. N., Sivasankari S. S., Surendiran J., et al., “Early Lung Cancer Prediction using Correlation and Regression,” Proc. Int. Conf. on Computer Power and Communications, pp. 24–28, 2022. https://doi.org/10.1109/ICCPC55978.2022.10072059.

[17] Vidhya R. G., Seetha J., Ramadass S., Dilipkumar S., Sundaram A., Saritha G., “An Efficient Algorithm to Classify the Mitotic Cell using Ant Colony Algorithm,” Proc. Int. Conf. on Computer Power and Communications, pp. 512–517, 2022. https://doi.org/10.1109/IC-CPC55978.2022.10072277.

[18] Sengeni D., Muthuraman A., Vurukonda N., Priyanka G., et al., “A Switching Event-Triggered Approach to Proportional Integral Synchronization Control for Complex Dynamical Networks,” Proc. Int. Conf. on Edge Computing and Applications, pp. 891–894, 2022. https://doi.org/10.1109/ICE-CAA55415.2022.9936124.

[19] Vidhya R. G., Rani B. K., Singh K., Kalpanadevi D., Patra J. P., Srinivas T. A. S., “An Effective Evaluation of SONARS using Arduino and Display on Processing IDE,” Proc. Int. Conf. on Computer Power and Communications, pp. 500–505, 2022. https://doi.org/10.1109/ICE-CAA55415.2022.9936124.

[20] Kushwaha S., Boga J., Rao B. S. S., Taqui S. N., et al., “Machine Learning Method for the Diagnosis of Retinal Diseases using Convolutional Neural Network,” Proc. Int. Conf. on Data Science, Agents & Artificial Intelligence, 2023, pp. 1–. https://doi.org/10.1109/ICDSAAI59313.2023.10452440.

[21] Maheswari B. U., Kirubakaran S., Saravanan P., Jeyalaxmi M., Ramesh A., et al., “Implementation and Prediction of Accurate Data Forecasting Detection with Different Approaches,” Proc. 4th Int. Conf. on Smart Electronics and Communication, 2023, pp. 891–897. https://doi.org/10.1109/ICOSEC58147.2023.10276331.

[22] Mayuranathan M., Akilandasowmya G., Jayaram B., Velrani K. S., Kumar M., et al., “Artificial Intelligent based Models for Event Extraction using Customer Support Applications,” Proc. 2nd Int. Conf. on Augmented Intelligence and Sustainable Systems, 2023, pp. 167–172. https://doi.org/10.1109/ICAISS58487.2023.10250679.

[23] Gold J., Maheswari K., Reddy P. N., Rajan T. S., Kumar S. S., et al., “An Optimized Centric Method to Analyze the Seeds with Five Stages Technique to Enhance the Quality,” Proc. Int. Conf. on Augmented Intelligence and Sustainable Systems, 2023, pp. 837–842. https://doi.org/10.1109/ICAISS58487.2023.10250681.

[24] Anand L., Maurya J. M., Seetha D., Nagaraju D., et al., “An Intelligent Approach to Segment the Liver Cancer using Machine Learning Method,” Proc. 4th Int. Conf. on Electronics and Sustainable Communication Systems, 2023, pp. 1488–1493. https://doi.org/10.1109/ICESC57686.2023.10193190.

[25] Harish Babu B., Indradeep Kumar, et al., “Advanced Electric Propulsion Systems for Unmanned Aerial Vehicles,” Proc. 2nd Int. Conf. on Sustainable Computing and Smart Systems (ICSCSS), 2024, pp. 5–9, IEEE. https://doi.org/10.1109/ICSCSS60660.2024.10625489.

[26] Jagan Raja V., Dhanamalar M., Solaimalai G., et al., “Machine Learning Revolutionizing Performance Evaluation: Recent Developments and Breakthroughs,” Proc. 2nd Int. Conf. on Sustainable Computing and Smart Systems (ICSCSS), 2024, pp. 780–785, IEEE. https://doi.org/10.1109/ICSCSS60660.2024.10625103.

[27] Sivasankari S. S., Surendiran J., Yuvaraj N., et al., “Classification of Diabetes using Multilayer Perceptron,” Proc. IEEE Int. Conf. on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), 2022, pp. 1–5, IEEE. https://doi.org/10.1109/ICDCECE53908.2022.9793085.

[28] Anushkannan N. K., Kumbhar V. R., Maddila S. K., et al., “YOLO Algorithm for Helmet Detection in Industries for Safety Purpose,” Proc. 3rd Int. Conf. on Smart Electronics and Communication (ICOSEC), 2022, pp. 225–230, IEEE. https://doi.org/10.1109/ICOSEC54921.2022.9952154.

[29] Reddy K. S., Vijayan V. P., Das Gupta A., et al., “Implementation of Super Resolution in Images Based on Generative Adversarial Network,” Proc. 8th Int. Conf. on Smart Structures and Systems (ICSSS), 2022, pp. 1–7, IEEE. https://doi.org/10.1109/ICSSS54381.2022.9782170.

[30] Joseph J. A., Kumar K. K., Veerraju N., Ramadass S., Narayanan S., et al., “Artificial Intelligence Method for Detecting Brain Cancer using Advanced Intelligent Algorithms,” Proc. Int. Conf. on Electronics and Sustainable Communication Systems, 2023, pp. 1482–1487. https://doi.org/10.1109/ICESC57686.2023.10193659.

[31] Surendiran J., Kumar K. D., Sathiya T., et al., “Prediction of Lung Cancer at Early Stage Using Correlation Analysis and Regression Modelling,” Proc. 4th Int. Conf. on Cognitive Computing and Information Processing, 2022, pp. 1–. https://doi.org/10.1109/CCIP57447.2022.10058630.

[32] Goud D. S., Varghese V., Umare K. B., Surendiran J., et al., “Internet of Things-based Infrastructure for the Accelerated Charging of Electric Vehicles,” Proc. Int. Conf. on Computer Power and Communications, 2022, pp. 1–6. https://doi.org/10.1109/ICCPC55978.2022.10072086.

[33] Vidhya R. G., Singh K., Paul J. P., Srinivas T. A. S., Patra J. P., Sagar K. V. D., “Smart Design and Implementation of Self-Adjusting Robot using Arduino,” Proc. Int. Conf. on Augmented Intelligence and Sustainable Systems, 2022, pp. 1–6. https://doi.org/10.1109/ICAISS55157.2022.10011083.

[34] Vallathan G., Yanamadni V. R., et al., “An Analysis and Study of Brain Cancer with RNN Algorithm-based AI Technique,” Proc. Int. Conf. on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), 2023, pp. 637–642. https://doi.org/10.1109/I-SMAC58438.2023.10290397.

[35] Vidhya R. G., Bhoopathy V., Kamal M. S., Shukla A. K., Gururaj T., Thulasimani T., “Smart Design and Implementation of Home Automation System using Wi-Fi,” Proc. Int. Conf. on Augmented Intelligence and Sustainable Systems, 2022, pp. 1203–1208. https://doi.org/10.1109/ICAISS55157.2022.10010792.

[36] Vidhya R., Banavath D., Kayalvili S., Naidu S. M., Prabu V. C., et al., “Alzheimer’s Disease Detection using Residual Neural Network with LSTM Hybrid Deep Learning Models,” J. Intelligent & Fuzzy Systems, 2023; vol. 45, no. 6, pp. 12095–12109. https://doi.org/10.3233/JIFS-235059.

[37] Balasubramaniyan S., Kumar P. K., Vaigundamoorthi M., Rahuman A. K., et al., “Deep Learning Method to Analyze the Bi-LSTM Model for Energy Consumption Forecasting in Smart Cities,” Proc. Int. Conf. on Sustainable Communication Networks and Application, 2023, pp. 870–876 https://doi.org/10.1109/ICSCNA58489.2023.10370467.

[38] Somani V., Rahman A. N., Verma D., et al., “Classification of Motor Unit Action Potential Using Transfer Learning for the Diagnosis of Neuromuscular Diseases,” Proc. 8th Int. Conf. on Smart Structures and Systems (ICSSS), 2022, pp. 1–7, IEEE. https://doi.org/10.1109/ICSSS54381.2022.9782209.

[39] Vidhya R. G., Saravanan R., Rajalakshmi K., “Mitosis Detection for Breast Cancer Grading,” Int. J. Advanced Science and Technology, 2020; vol. 29, no. 3, pp. 4478–4485.

[40] Gupta D., Kezia Rani B., Verma I., et al., “Metaheuristic Machine Learning Algorithms for Liver Disease Prediction,” Int. Res. J. Multidisciplinary Scope, 2024; vol. 5, no. 4, pp. 651–660. https://doi.org/10.47857/irjms.2024.v05i04.01204.

[41] Sudhagar D., Saturi S., Choudhary M., et al., “Revolutionizing Data Transmission Efficiency in IoT-Enabled Smart Cities: A Novel Optimization-Centric Approach,” Int. Res. J. Multidisciplinary Scope, 2024; vol. 5, no. 4, pp. 592–602. https://doi.org/10.47857/irjms.2024.v05i04.01113.

[42] Vidhya R. G., Batri K., “Segmentation, Classification and Krill Herd Optimization of Breast Cancer,” J. Medical Imaging and Health Informatics, 2020; vol. 10, no. 6, pp. 1294–1300. https://doi.org/10.1166/jmihi.2020.3060.

[43] Carboni D., “Feedback-based Reputation on Top of the Bitcoin Blockchain,” arXiv preprint, 2015; arXiv:1502.01504.

[44] Alcaraz C., Roman R., Najera P., Lopez J., “Security of Industrial Sensor Network-Based Remote Substations in the Context of the Internet of Things,” Ad Hoc Networks, 2013; vol. 11, no. 3, pp. 1091–1100. https://doi.org/10.1016/j.adhoc.2012.12.001.

[45] Arbaugh W., Farber D., Smith J., “A Secure and Reliable Bootstrap Architecture,” Proc. IEEE Symp. on Security and Privacy, 1997, pp. 100–116.

[46] Xu Z, Yang Y, Liu J, Chen C, Zhang T. Federated Learning in Biomedicine: Current Status, Challenges, and Opportunities. IEEE Transactions on Industrial Informatics. 2021; 17(6):4473-4481.

[47] Siddiqui JH, Ahmad R, Patel S, Khan M, Ali J. Data Fusion in Deep Learning Models for Breast Cancer Staging Prediction: A Comprehensive Study. IEEE Access. 2020; 8:108844-108857.