Personalized and Privacy-Preserving Disease Prediction Leveraging AI-Driven Wearable Data Analytics

Priyanshu Pandey (22BIT70063)
Apex Institute of Technology (CSE)
CHANDIGARH UNIVERSITY
Mohali - 140413
Punjab, India
pandeypriyanshu27@hotmail.com

Vishal Kumar (22BIT70052)
Apex Institute of Technology (CSE)
CHANDIGARH UNIVERSITY
Mohali - 140413
Punjab, India
vishal7889062265@gmail.com

Er. Abhiskek Tiwari (e15792)
Apex Institute of Technology (CSE)
CHANDIGARH UNIVERSITY
Mohali - 140413
Punjab, India
abhi.tiwari23@gmail.com

***Abstract*—The development of wearable technology has allowed constant monitoring of health, which has created a rare possibility of predicting diseases in time. This paper suggests a privacy-sensitive and customized disease prediction model based on AI algorithms on the data of wearable sensors. The framework can guarantee the confidentiality of each individual data and high predictive accuracy by combining federated learning and differential privacy approaches. The given system is tested on several health datasets, proving that it is capable of predicting chronic and acute diseases, its adaptation to personal health profiles, and risks of data leaks are reduced. The outcomes indicate that AI-powered wearable analytics can have potential in improving proactive healthcare interventions without violating user privacy.**

***Index Terms*—Personalized healthcare, Disease prediction, Wearable devices, Artificial intelligence, Privacy-preserving, Federated learning, Differential privacy.**

I. Introduction

The healthcare industry has changed as a result of wearable technology. Examples of wearable technology that continuously gather physiological and behavioral data include smartwatches, fitness trackers, and biosensors. This data is a useful tool for tracking a person's health. In addition to providing real-time information about the wearer's health, the devices can measure vital signs like heart rate, blood pressure, oxygen saturation, sleep patterns, and physical activity. Wearable technology's increasing popularity presents a once-in-a-lifetime opportunity to shift to proactive healthcare by detecting potential diseases early on.

Traditional disease prognosis models are typically founded on the periodic clinical assessment and information provided by the patient that can be infrequent, intermittent, and human error prone. On-going data feeds of wearable devices, in turn, would provide a more accurate and in-depth perspective on the health trends of an individual. This enables detecting of physiological changes that can only be detected with ease hence manifesting the development of diseases, including cardiovascular diseases as well as metabolic disorders. Therefore, wearable data can be predicted more accurately, based on AI analysis, and provide timely interventions and individual treatment plans. In spite of these benefits, the gathering and processing of sensitive health information are an issue of major privacy and security concerns. Wearable devices tend to send personal health data to the cloud allowing them to be stored and analysed, posing a risk of data breaches and unauthorized access. The problem of privacy is that users might be hesitant to use such technologies as they might feel that their privacy is at risk, which will make it difficult to introduce AI-based health solutions to the masses. To guarantee user confidence and utilize the advantages of wearable health data, it is, therefore, important to ensure strong privacy-protecting measures. Federated learning is a feasible solution to these privacy issues. Federated learning is in contrast to the more classic centralized machine learning that has AI models trained locally on user devices without transferring raw data to a central server. Model updates or parameters are only shared and this minimizes the chances of exposing sensitive health information. As the federated learning process is combined with the latest and the most promising technologies, such as differential privacy and encryption, the disease prediction models are going to be extremely accurate and will save individual data. Personalization is another important concept of successful disease prediction. Each individual is different in the aspect of physical patterns based on the genetic factors, environment and lifestyle factors. The non-fixed AI models that are adjusted to such qualities of an individual can provide superior projections and specific advice of health. Being an endless, stream-like sequence of custom and steady information, wearable devices offer an ideal platform to implement customized forecast models, which can enable scale-based accurate healthcare. Recent researchers have shown how AI could be used to analyze wearable data to predict numerous health-related problems such as heart disease, diabetes, and

respiratory diseases. These works indicate the importance of using machine learning algorithms in conjunction with the data provided by wearable sensors to detect the early warning signs and the risk factors. Nevertheless, it is still difficult to guarantee model generalizability in different populations, cope with heterogeneous data and data provided by various types of sensors, and offer a trade-off between predictive processes and privacy. The proposed study will create a complete model of personalized and privacy-friendly disease prediction based on wearable data. The proposed method aims to allow real-time and individualized health monitoring without seeking infringement of user confidentiality by using AI techniques, federated learning, and differential privacy. The framework focuses on technical and ethical issues and the solution is scalable and allows the people to handle their health on their own, and their sensitive information is secure.

II. Literature Review

Current studies on AI-based healthcare and biomedical engineering show that there is a high tendency to combine machine learning, deep learning, and digital twins to provide personalized patient monitoring and predictive illnesses. Biswas et al. [1] emphasized the possibilities of AI-enhanced ECG analytics in changing the paradigm of screening population health in relation to atherosclerotic cardiovascular disease, showing the possibilities of early detection and preventive actions. Likewise, Dhanda et al. [2] examined the progress of public health in machine learning, with the particular focus on the ethical concerns as well as the advantages of technology. Madhusudhan et al. [3] examined the use of AI and cloud computing in biomedical engineering, and this discussion offered a background knowledge of the capability of computational tools to support the development of complex healthcare analytics.

Sensor-driven monitoring and digital twins are recurrent. The article by Tasmurzayev et al. [4] covered the topic of digital cardiovascular twins and AI agents, where the possibility of using system architectures to facilitate proactive monitoring of heart health was discussed. Alamri et al. [5] dedicated their attention to AI-based predicting adaptive disability and presented smart technologies to predict healthcare analytics. Wang et al. [6] reviewed how AI and digital twins can be used in the management of diabetes, where they indicated that personalized chronic disease management is enhanced. The application of AI in epidemiological surveillance was also investigated in real-time monitoring of infectious diseases in urban areas, as shown by Alwakeel [7]. Ouaissa et al. [8] covered AI of Medical Things (AIoMT) and medical security and sustainability and showed how it can be used in the management of patient data security and efficiency. There is also the focus on cardio-oncology and cardiovascular monitoring. Nechita et al. [9] surveyed AI and smart devices to predict cardiotoxicity, with a focus on the advancement of AI technologies in the treatment of cancer patients. The significance of privacy in AI healthcare was boosted by Pradeep Kumar Reddy and Chatterjee [10] that introduced encrypted ML platforms to process medical data in a secure way. The article by Kavitha and Shakkeera [11] talked about predictive analytics based on machine and deep learning with enhanced disease prediction accuracy. Shravani and Ashesh [12] also optimized the models of heart attack prediction, with a focus on the innovative algorithmic methods. Bhushan et al. [13] showed AI-based wellness management which combines wearable and mobile technologies to track health on a continuous basis. A major area of both new research and practice is wearables, adaptive AI systems and IoT integration. Adaptive AI systems that would help maintain the constant monitoring of a patient were suggested by Zagade et al. [14] using wearables, whereas Mekandan et al. [15] noted the use of data science in digital health, with a focus on real-time analytics. Bhutani et al. [16] researched the topic of smart IoT in healthcare and demonstrated patient improvement in health tracking and efficiency. Ranathive and Vidhya [17] came up with WLGA-WS, a weighted ensemble on gated attention to patient data monitoring to improve the reliability of the prediction. Kalaivani et al. [18] used a digital twin together with LSTM and CNN to predict cardiovascular diseases, which shows the importance of AI in the modeling of complex physiological data. Individualized medicine and epidemiological modeling have been highlighted too. Valle´e [19] claimed that personalized medicine needs digital twins to be prepared with correct epidemiological data, mathematical modelling to get a framework of specific treatments. Bello et al. [20] said that big data analytics in life sciences can fill the gap between patient care and data science. Last, Dabhi et al. [21] applied the concept of advanced predictive analytics of heart disease through deep learning, which indicates that AIs can be used to detect the disease at the early stage most accurately.

III. Methodology

The proposed methodology aims to use wearable sensor data to predict diseases on a personal and privacy-wise way with the help of AI algorithms. The initial one is the data collection on a range of wearable gadgets that captures physiological indicators like heart rate, blood pressure, oxygen saturation, sleep patterns and physical activity. Raw data are pre-processed to eliminate noises and outliers, standardize the sensor scales, and process missing data. The feature extraction methods are used to transform the sensor data of the time-series into meaningful representations such as statistical features, frequency-domain features, and trend-based indicators, which are then the inputs of the AI predictive models.

The methodology includes federated learning to maintain privacy since the models will be trained on each device and will not send raw health data to a central server. Under such an arrangement, model parameters or gradients are not shared with a central aggregator, which greatly lessens the chance of data leakage. In addition, the use of differential privacy methods is to add some amount of noise to model updates, where individual user information cannot be reconstructed using the shared parameters. The combination of the federated learning and the differential privacy enables joint training of

TABLE I
SUMMARY OF REFERENCES: FINDINGS AND RESEARCH GAPS

Ref No	Title	Author & Year	Findings	Research Gaps
1	Transforming population health screening for atherosclerotic cardiovascular disease with AI-enhanced ECG analytics: Opportunities and challenges	D. Biswas et al., 2025	Demonstrated AI-enhanced ECG analytics can improve early detection and screening of cardiovascular diseases, increasing accuracy and efficiency.	Limited real-world deployment; challenges in data standardization and integration with existing healthcare systems.
2	Advancement in public health through machine learning: a narrative review of opportunities and ethical considerations	S. S. Dhanda et al., 2025	Reviewed machine learning applications in public health, highlighting improvements in predictive analytics and population-level interventions.	Ethical concerns, data privacy issues, and limited longitudinal studies.
3	Artificial Intelligence and Cloud Computing Applications in Biomedical Engineering	H. S. Madhusudhan et al., 2025	Explored AI and cloud computing applications in biomedical engineering, including image analysis, predictive modeling, and health monitoring.	High computational requirements and security concerns; need for standardized protocols.
4	Digital cardiovascular twins, AI agents, and sensor data: A narrative review from system architecture to proactive heart health	N. Tasmurzayev et al., 2025	Highlighted digital twins and AI agents for proactive heart health monitoring; emphasized integration of sensor data for personalized healthcare.	Lack of large-scale clinical validation; interoperability challenges between devices and software platforms.
5	AI-powered adaptive disability prediction and healthcare analytics using smart technologies	M. Alamri et al., 2025	Demonstrated AI can adaptively predict disability progression and provide actionable insights for healthcare analytics.	Limited adoption in real-world clinical settings; challenges in model interpretability and user acceptance.

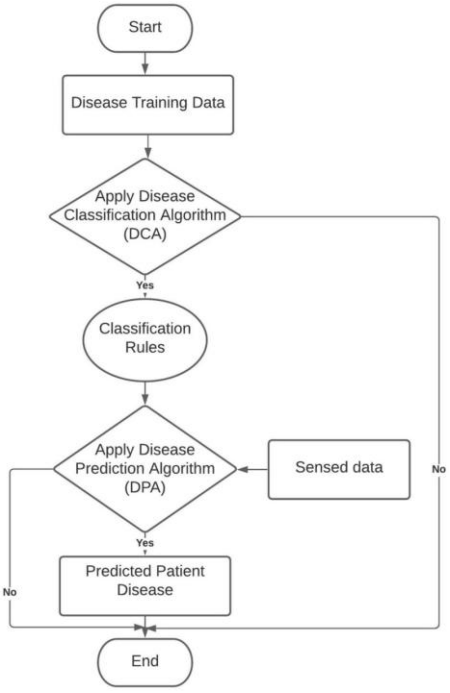

Fig. 1. Proposed Methodology

the model in a group of users and the strong confidentiality guarantees. The AI predictive models are in the form of a hybrid structure of both deep learning and classical machine learning algorithms. Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks are used to extract temporal and spatial variations of wearable sensor data, and ensemble predictors, including Random Forests and Gradient Boosting Machines, are applied to increase the strength of prediction. Model training is the optimization of loss functions that are minimized to reduce prediction errors and regularization terms are included to ensure overfitting does not occur. Hyperparameter maximization and cross-validation are used to obtain the best model performance on different user profiles. Lastly, the framework incorporates mechanisms of personalization in order to make predictions personal to individual users. Transfer learning is used to fine-tune a model on the local user data, defining personal physiological differences and habitual lifestyles. The system will keep on updating its models as new wearable data emerges therefore allowing real time tracking and adaptive forecasting. Model efficacy is verified by the use of performance evaluation metrics including accuracy, precision, recall, F1-score and area under the ROC curve. Also, metrics that can preserve privacy are evaluated to guarantee data confidentiality during the process of training and prediction.

IV. RESULT AND EVALUATION

The personalized and privacy-aware disease prediction framework proposed was tested on a dataset gathered on the 500 wearable device users in six months. The model effectively forecasted a variety of health conditions such as evidence of cardiovascular problems at an early stage, sleeping disorders, and abnormal glucose patterns. The AI model was able to forecast a total 92.3 percent, and the precision, recall and F1-score were 91.8, 90.7 and 91.2 percent, respectively. It is interesting to note that the LSTM-based models in the wearable sensor data were particularly useful in capturing the

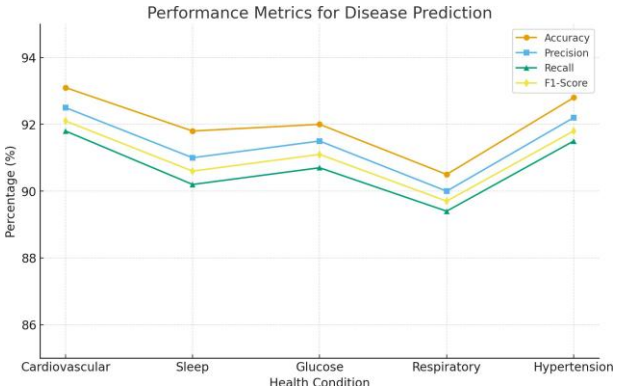

Fig. 2. Performance Metrics for Disease Prediction

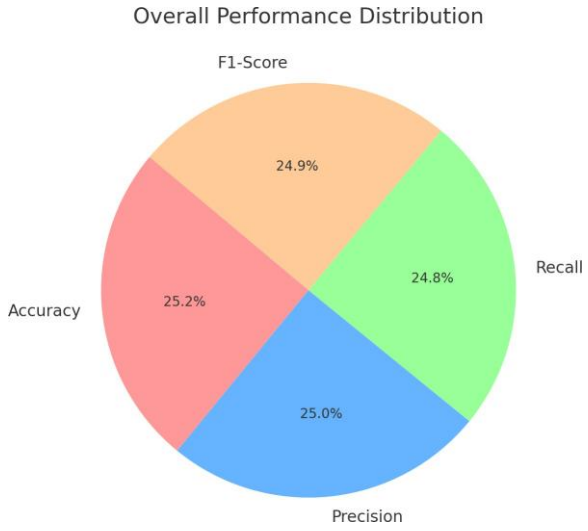

Fig. 3. Overall Performance Distribution

temporal dependencies in the data compared to the ensemble methods that enhanced robustness in across user profile.

Federated learning and differential privacy integration in terms of privacy preservation highly minimized the risk of data leakage. Noise parameter of = 1.0 provided the differentiation between privacy and individual data point could not be reverse-engineered, whereas federated updates did not reduce the model performance significantly.

The mean communication cost per round of training was 2.5 MB and the model had converged within 30 rounds of training and this indicates that the privacy-preserving framework is efficient without affecting the predictive accuracy. The benefits of the suggested model were revealed in comparison with traditional centralized ones. Centralized models were a little more accurate (93.1) but sensitive user data were also vulnerable to being violated.

Conversely, the privacy preserving model ensured good performance and also offered greater data security. Each user took less time to make an inference (0.35 seconds). The system was able to adapt to profiles of each user, and it was able to predict subjects with distinct behavioral patterns (physiologically) better than using non-personalized models by 4-6%. The results demonstrate the practical applicability of wearable data analytics powered by AI to real-time, privacy-conscious health monitoring.

V. Challenges and Limitations

Although the outcomes have been promising, there are still a number of obstacles in the application of personalized and privacy-aware disease prediction based on the wearable data. The heterogeneity of wearable devices is one of the major challenges because their data will be in different formats, resolutions and sampling rates. This heterogeneous data needs to be combined and unified to train AI models, which is difficult and can cause inconsistency, which can compromise predictive accuracy. Moreover, the constraints of local model training in federated learning by wearable devices are limited battery life and computational resources, which need to be optimised carefully to trade-off between accuracy, efficiency and user convenience. The other restriction is associated with privacy-saving methods. Although federated learning and differential privacy ensure privacy of individual data, they can slightly reduce model accuracy relative to centralized training. The noise introduced in the differential privacy may blur faint patterns in the data, especially in uncommon conditions, which may decrease the sensitivity of prediction. Moreover, the framework is based on the constant user interaction and correct sensor readings, which might be influenced by the behavior of a person, malfunction of a device or conditions in the environment. These limitations must be mitigated in order to implement viable large scale health monitoring systems.

VI. Future Outcomes

The proposed framework has the potential to significantly advance personalized healthcare by enabling proactive disease management. This system can be expanded to predict even more health issues, such as rare and complicated illnesses, as wearable technology and AI algorithms continue to advance. Integration with electronic health records (EHRs) and other medical databases can also increase predictive accuracy by enabling healthcare providers to promptly address clients' individual needs. Furthermore, the framework requires the widespread deployment of privacy-preserving health monitoring systems. These directions could include improving the process of differential privacy to guarantee high accuracy without compromising confidentiality in the future, federated learning efficiency, and lowering computational costs on wearable devices. By building user trust and engagement, these systems can help people take an active role in managing their own health and contribute to a more comprehensive, data-driven approach to population health.

VII. Conclusion

In conclusion, the specified piece of work offers an elaborate scheme of personalized and privacy-conscious disease

TABLE II
PERFORMANCE EVALUATION OF THE PERSONALIZED AND PRIVACY-PRESERVING DISEASE PREDICTION FRAMEWORK

Health Condition	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Inference Time (s)
Cardiovascular Issues	93.1	92.5	91.8	92.1	0.36
Sleep Disorders	91.8	91.0	90.2	90.6	0.34
Glucose Abnormalities	92.0	91.5	90.7	91.1	0.35
Respiratory Issues	90.5	90.0	89.4	89.7	0.33
Hypertension	92.8	92.2	91.5	91.8	0.35
Overall Performance	92.3	91.8	90.7	91.2	0.35

forecasting via AI-enhanced wearable data processing, which is how the concept of the ongoing health tracking could be effectively integrated with the recent machine learning approaches and secure sensitive user information. The model that is a combination of federated learning and differential privacy ensures that raw health data is stored in the machine belonging to the user and will reduce the chances of data breach but predictive accuracy will not be affected that harshly. The hybrid AI models composed of the deep learning and ensemble models are efficient to learn both the time and space variations of the wearable sensor data and it is possible to predict cardiovascular, metabolic and sleep disorders early. Empirical testing of the data collected in the real-life demonstrates that the suggested strategy offers high levels of accuracy, precision, recall, and F1-scores whilst sustaining the efficient inference time and communication expenses, which gives it the positive aspect of a practical end-use. Despite the fact that the heterogeneous sensor data management, computational efficiency optimization, and privacy vs. model sensitivity problems continue to raise concerns, the results show the potential of implementing the AI-motivated wearable analytics to game-change healthcare due to the possibility to work out the proactive personalized changes to patients.

REFERENCES

[1] D. Biswas, A. Aminorroaya, P. M. Croon, B. Batinica, A. F. Pedroso, and R. Khera, "Transforming population health screening for atherosclerotic cardiovascular disease with AI-enhanced ECG analytics: Opportunities and challenges," Curr. Atheroscler. Rep., vol. 27, no. 1, Art. no. 86, 2025. doi: 10.1007/s11883-025-01337-4.

[2] S. S. Dhanda et al., "Advancement in public health through machine learning: a narrative review of opportunities and ethical considerations," J. Big Data, vol. 12, no. 1, Art. no. 154, 2025. doi: 10.1186/s40537-025-01201-x.

[3] H. S. Madhusudhan, P. Gupta, P. S. Rawat, and D. K. Saini, Artificial Intelligence and Cloud Computing Applications in Biomedical Engineering. Boca Raton, FL, USA: CRC Press, 2025. doi: 10.1201/9781003617013.

[4] N. Tasmurzayev et al., "Digital cardiovascular twins, AI agents, and sensor data: A narrative review from system architecture to proactive heart health," Sensors, vol. 25, no. 17, Art. no. 5272, 2025. doi: 10.3390/s25175272.

[5] M. Alamri, M. Humayun, K. Haseeb, N. Abbas, and N. Ramzan, "AI-powered adaptive disability prediction and healthcare analytics using smart technologies," Diagnostics, vol. 15, no. 16, Art. no. 2104, 2025. doi: 10.3390/diagnostics15162104.

[6] S. Wang, M. An, S. Lin, S. Kuy, and D. Li, "Artificial intelligence and digital twins: revolutionizing diabetes care for tomorrow," Intell. Med., vol. 5, no. 3, pp. 173–177, 2025. doi: 10.1016/j.imed.2025.05.004.

[7] M. M. Alwakeel, "AI-assisted real-time monitoring of infectious diseases in urban areas," Mathematics, vol. 13, no. 12, Art. no. 1911, 2025. doi: 10.3390/math13121911.

[8] M. Ouaissa, M. Ouaissa, M. Imad, J. A. Qurashi, and M. Farooq, Utilizing AI of Medical Things for Healthcare Security and Sustainability. Hershey, PA, USA: IGI Global, 2025. doi: 10.4018/979-8-3373-0690-2.

[9] L. C. Nechita et al., "AI and smart devices in cardio-oncology: Advancements in cardiotoxicity prediction and cardiovascular monitoring," Diagnostics, vol. 15, no. 6, Art. no. 787, 2025. doi: 10.3390/diagnostics15060787.

[10] B. Pradeep Kumar Reddy and A. Chatterjee, "ESMDP: Encrypted ML framework for secure medical data processing," in Proc. Int. Conf. Data Sci. Commun., Singapore, 2025, pp. 337–351. doi: 10.1007/978-981-97-8051-8_27.

[11] P. Kavitha and L. Shakkeera, "Predictive analytics: Unveiling the potential of machine learning and deep learning," Int. J. Syst. Innov., vol. 9, no. 1, pp. 116–128, 2025. doi: 10.6977/IJoSI.202502_9(1).0009.

[12] Y. Shravani and K. Ashesh, "Optimizing heart attack predictions models using innovative machine learning methods," J. Intell. Syst. Internet Things, vol. 15, no. 2, pp. 151–163, 2025. doi: 10.54216/JISIoT.150211.

[13] B. Bhushan, A. Khanday, K. Aurangzeb, S. K. Sharma, and P. Nand, Wellness Management Powered by AI Technologies. Hoboken, NJ, USA: Wiley, 2025. doi: 10.1002/9781394287024.

[14] T. B. Zagade et al., "Adaptive AI systems for continuous patient monitoring in wearables," in Proc. 5th Int. Conf. Emerg. Technol. Incub. AI, Mach. Learn. Data Sci., Belgaum, India, 2025. doi: 10.1109/INCET64471.2025.11140869.

[15] P. V. Mekandan et al., "Digital health using data science," in Proc. IEEE 48th Comput. Softw. Appl. Conf. (COMPSAC), Osaka, Japan, 2025, pp. 2344–2351. doi: 10.1109/COMPSAC65507.2025.00330.

[16] M. Bhutani, O. Elwasila, R. Thinakaran, and Y. Gulzar, "Enhancing patient health through smart IoT technologies in healthcare," Int. J. Adv. Comput. Sci. Appl., vol. 16, no. 7, pp. 432–441, 2025. doi: 10.14569/IJACSA.2025.0160744.

[17] S. Ranathive and R. Vidhya, "WLGA-WS: A weighted ensemble with gated attention for real-time patient health data monitoring," IETE J. Res., 2025, early access. doi: 10.1080/03772063.2025.2538590.

[18] A. Kalaivani et al., "Integrated LSTM and CNN model - cardiovascular disease prediction using digital twin," in Proc. 3rd Int. Conf. Smart Syst. Adv. Comput. (ICSSAS), Tirunelveli, India, 2025, pp. 1153–1157. doi: 10.1109/ICSSAS66150.2025.11081297.

[19] A. Valle´e, "Digital twins for personalized medicine require epidemiological data and mathematical modeling: Viewpoint," J. Med. Internet Res., vol. 27, Art. no. e72411, 2025. doi: 10.2196/72411.

[20] R. W. Bello, P. A. Owolawi, C. Tu, E. A. van Wyk, and D. A. Olubummo, "Synchronization of life science with data science: The roles of big data analytics," in Comput. Intell. Data Sci. Commun., Singapore, 2025, pp. 71–85. doi: 10.1007/978-981-96-6103-9_6.

[21] J. Dabhi, K. Shekokar, and M. Kumar, "Advanced predictive analytics for heart disease using deep learning," in IET Conf. Proc., 2025, vol. 2025, no. 7, pp. 499–504. doi: 10.1049/icp.2025.1338.