AI-Powered IoT Framework for Predictive Maintenance and Fault Detection in Healthcare Devices

Varsha Negi[1], R. Ravi[2], Venkata Ramana Banka[3], S. Jeeva[4], Vikram P.[5] and Syed Zahidur Rashid[6]
[1]Department of Computer Science, Shyam Lal College Evening, Shahdara, Delhi University, Delhi 110032, India
[2]Department of Information Technology, J. J. College of Engineering and Technology, Tiruchirappalli, Tamil Nadu, India
[3]Department of Computer Science and Engineering (AIML), CVR College of Engineering, Hyderabad 501510, Telangana, India
[4]Department of Management Studies, Nandha Engineering College, Vaikkalmedu, Erode - 638052, Tamil Nadu, India
[5]Department of CSE, New Prince Shri Bhavani College of Engineering and Technology, Chennai, Tamil Nadu, India
[6]Department of Electronic and Telecommunication Engineering, International Islamic University Chittagong, Chittagong, Bangladesh

Keywords: an IoT, Predictive Maintenance, Healthcare Devices, Fault Detection, Explainable AI.

Abstract: In the age of digitized healthcare, maintaining and monitoring the operational effectiveness and reliability of biomedical devices is fundamental to patient security and clinical effectiveness. Consequently, this article provides a Secure & Scalable AIoT Framework for Real-Time Predictive Maintenance and Ethical Fault Detection in Healthcare Devices that combines the concepts of AI and the Internet of Things (AIoT) to realise intelligent monitoring, fault prediction and proactive maintenance. Specifically, the introduced framework addresses critical limitations in today's systems by integrating high-precision data verification modules, strong inter-operability via healthcare data standards and privacy-preserving AI models in accordance with HIPPA and GDPR regulations. Thus lightweight accurate machine learning algorithms are used for low-power, resource-constraint IoT devices, providing scalability and efficiency when potentially operating in event environments with real-time analytics. Also, the framework observes ethical AI procedural using explainable AI (XAI) and bias-mitigation techniques to ensure reliance and trust in critical decision making. Through predictive alerts and visual insights, a user-centric dashboard enables the clinical workforce to act in a timely manner. The system's modular architecture allows adaptive deployment across various healthcare infrastructures, providing a comprehensive solution for intelligent device management that is future-ready. Through experimental evaluations, we provide compelling evidence of marked improvements in fault detection accuracy, prediction latency, and data security, validating its practicality for real-world clinical use.

1 INTRODUCTION

The explosion of digital transformation in healthcare has opened the doors to a new era where artificial intelligence (AI) and the Internet of Things (IoT) have begun to reshape the landscape of patient wellness, service experience, device durability and operational excellence. Medical devices which include everything from ventilators to infusion pumps to wearable monitors are central to today's clinical workflows, and any unexpected failure can result in postponed treatments, higher costs or even life-threatening situations. In such high-stakes environments, however, conventional maintenance strategies such as reactive and scheduled servicing are becoming increasingly inadequate, frequently noting indications of device deterioration too late. To surmount these drawbacks, this paper presents a Secure and Scalable AIoT Framework for Real-Time Predictive Maintenance and Ethical Fault Detection in Healthcare Devices. By utilizing actual data feeds from Internet of Things (IoT) connected medical devices and utilizing sophisticated AI models, it enables anomaly detection, potential failure forecasting, and proactive maintenance actions. In contrast to conventional systems, we propose a framework that embeds high-integrity data pipelines

Negi, V., Ravi, R., Banka, V. R., Jeeva, S., P., V. and Rashid, S. Z.
AI-Powered IoT Framework for Predictive Maintenance and Fault Detection in Healthcare Devices.
DOI: 10.5220/0013867800004919

In *Proceedings of the 1st International Conference on Research and Development in Information, Communication, and Computing Technologies (ICRDICCT'25 2025) - Volume 1*, pages 468-477
ISBN: 978-989-758-777-1

that have embedded validation mechanisms toward ensuring consistent and reliable input to the learning models. Additionally, the aircraft integrates more than just the technical aspects; it enshrines ethical AI principles with explanation, equity, and privacy. Using federated learning, differential privacy, and regulatory standards such as HIPAA and GDPR compliance, the framework guarantees safe handling of sensitive patient-device data. Its lightweight architecture offers productized deployability on low-power edge devices, enabling it to be a fit for diverse healthcare settings from massive hospitals to mobile clinics.

Visual analytics combined with a unified dashboard equips clinical and technical personnel to screen device wellness perceptively, catch actionable insights and answer maintenance signals ahead of time. The solution is modular and interoperable, so it can be adapted to diverse healthcare IT ecosystems, resulting in scalability and future-proofing of the solution for widespread adoption.

We detail the system design, implementation, and evaluation of the proposed framework. Comprehensive experiments confirm its effectiveness in terms of real-time fault detection, predictive maintenance, high model interpretability and data security, thus providing a robust foundation for the next generation of intelligent medical device management systems.

2 PROBLEM STATEMENT

As smart medical devices and IoT-enabled equipment becomes more prevalent in the healthcare ecosystem, this dependence presents problems in ensuring these systems remain reliable and safe and their availability. Conventional maintenance strategies, including regular inspections and reactive servicing, are becoming inadequate to the needs of modern healthcare environments, where the consequences of device failure can be severe, even life-threatening. Unexpected failures in devices such as infusion pumps, ventilators, ECG monitors or diagnostic equipment can result in delays in treatment, compromised patient outcomes and additional operational costs.

While many predictive maintenance models have been established in the literature, most current frameworks have critical limitations, including poor data quality resulting from sensor unreliability, inability to process data in real-time, inefficient integration with healthcare IT standards, and a lack of approaches that support data privacy and ethical AI practices. Furthermore, very few systems can effectively scale across varied healthcare infrastructures or run seamlessly on low-power IoT devices.

The remaining issue is that with no explainable AI mechanisms in place, clinicians and technicians cannot trust or understand the predictions, which hampers clinical decision-making. In particular, the failure to comply with regulations and ensure safe handling of data aggravates these problems, since interconnected medical devices will generate and transfer sensitive patient data.

Therefore, it is essential to develop a secure, scalable, and ethically-grounded AI-driven IoT framework that enables real-time fault detection and predictive maintenance of physical systems while maintaining data privacy, transparency, and operational efficiency. Given that this research intends to fill this gap, we propose a comprehensive and domain-specific approach that fits the characteristics of the complex needs of the healthcare ecosystem.

3 LITERATURE REVIEW

Artificial Intelligence (AI) combined with the Internet of Things (IoT) known as an IoT has become a major tool for achieving predictive maintenance and fault detection in mission-critical systems, particularly in healthcare. With medical equipments becoming more digitized and connected, the need for smart maintenance frameworks is becoming more prominent.

Pech et al. 2 Rashid et al. (2021) In smart factory settings, Rashid et al. (2021) argue for intelligent sensors and predictive analytics, highlighting the ability of AI-based maintenance strategies to minimize operational downtimes and expenses. Although this is an industrial setting, the principles are translatable into the healthcare world, where the stakes that is, patient safety are so much higher.

AI-based predictive maintenance systems: Key factors of trustworthiness (Ucar, Karakose, Kırımça, 2024) This work exposed gaps (explainability, trust, data integrity) between existing political models and systems developed for social media content, an issue that this paper address through ethical AI integrations and privacy-preserving architectures.

In their paper Sandu (Sandu (2022)) focused on AI driven framework for the predictive Maintainence of the Industrial IoT. His approach relied on fault prediction based on real-time anomaly detection algorithms but has not sufficiently focused on

healthcare-specific needs, such as the sensitivity of patient data, or the inter-operability of devices, topics that are comprehensively addressed in this study.

Khalid (2024) explored the use of AI-enabled digital transformation in the sustainable operations arena. His focus on scalability and energy-efficient design resonates with the lightweight model design of this paper that allows deployment on resource-constrained medical IoT devices.

He et al. (2019) studied how AI technologies can be implemented in real-world medicine, identifying regulatory, technical and ethical challenges preventing AI uptake. Informed by this understanding, the present work incorporates privacy techniques that are compliant with GDPR/HIPAA and explainable AI tools to engender trust in clinicians.

Dhameliya and Patel presented the predictive maintenance of general IoT systems using the machine learning models. However, their solution failed to tackle challenges such as interoperability with Electronic Health Record (EHR) systems or deployment in edge environments gaps that this research intends to fill.

Shajahan and Ramesh: An IoT health monitoring system with predictive analysis (2019). This was effective for real-time monitoring; however, it did not provide for scalability or ethical AI features, again highlighting the need for a more holistic framework as presented in this paper.

Pesapane et al. (2018) analyzed regulatory questions for using AI as a medical device, highlighting ethical dangers and legal ambiguities. However, our proposed framework comes to overcome them by embedding regulatory compliance in the design process and guaranteeing explainable decisions.

According to Pessin (2025), the role of connected devices in predictive diagnostics is expanding. His piece describes how these networked medical devices help reduce risk to patients through monitoring in real time. This paper extends that work to propose a secure system for large-scale such monitoring.

Davies (2025) studied the race for hospitals to go 'smart' with AI and IoT. He cited concern, however, around scalability and standardization — which this framework explicitly addresses through modular, standards-compliant architecture.

Focusing on Intelligent Transportation Systems, Iyer (2021) provided some key insights in edge deployment and resource aware AI design, which are also applied by this framework to achieve efficient semantic processing over medical devices.

From an industry perspective, Goja (2022) presented the AIoT architecture design and emphasized adaptability and interoperability. Our work realizes this vision in the healthcare vertical characterized as an end to end view across devices, and instant insights that span diverse grid infrastructure across a hospital.

Huber-Straßer et al. (2018) imagined the future value chains of robotics and AI. Albeit speculative, their focus on ethical frameworks and human-machine trust dovetails nicely with this research's aim of integrating fairness and interpretability into healthcare AI.

As Ghosh (2020) discussed, when AI and IoT integrate we get AIoT, but true real-time intelligence at the edge is needed. The proposed research widens the basis of that application by using a mendacious AIoT in high subsidiarity clinical settings with protection privacy and decision transparency.

Lin et al. (2019) showcased the AIoT applications by smart agriculture that indirectly verify the cross-domain applicability of AIoT models. This data-driven approach led us to develop a multi-tier data validation mechanism with a focus on high prediction accuracy in this paper.

Chu et al. (2019) reviewed AIoT in sports science, demonstrating that AIoT has the ability to monitor performance metrics instantaneously. We extend these principles in this work to monitor medical device status and failure trends within clinical settings.

Anumandla (2018) introduced a simplified predictive maintenance approach based on IoT and machine learning. Yet it did not possess a privacy model and explainability framework, which this paper combines to address healthcare applications.

Singh (2025) provided an overview of AI-driven sensors for predictive maintenance, including context-aware sensing. This notion of sensor fusion is the strategy we adopted in our system to extract operational and environment data of devices.

Cheng et al. In line with this concept, Dey et al. (2019) proposed an edge based AIoT system that supports real-time analytics and this architectural decision was also following in this work to reduce latency, and dependability on centralized servers.

Lin et al. It presented a new perspective that describes how low-latency decision-making inside AIoT improves system responsiveness (2019). Their model motivated our system's use of lightweight and edge-optimized models for real-time error notifications.

Pessin (2025) and Davies (2025) addressed industry level phenomena regarding predictive

diagnostics and reiterated the need for fault resilient critical systems, which we provide in our framework through integrated predictive alerts and maintenance scheduling.

Khalid (2024) and Ucar et al. (2024) singled out a lack of explainability in traditional models. This study directly responds to that gap with Explainable AI (XAI) tools like SHAP, which provide insights into model predictions in an interpretable manner.

Dhameliya & Patel (2020) and Shajahan & Ramesh (2019) considered general IoT environments but did not provide specialization for healthcare. Paper extends their foundation into a specialized, regulation compliant, healthcare framework.

4 METHODOLOGY

This section presents the methodology adopted for the development of a Secure and Scalable AIoT Framework for predictive maintenance and fault detection in healthcare devices. The approach combines AI, IoT, edge computing, and explainable AI (XAI) within a modular architecture that ensures real-time data processing, device interoperability, and adherence to privacy regulations.

4.1 Framework Design

The framework is built around the integration of IoT-enabled healthcare devices with AI-powered models for fault detection and maintenance prediction. Key components include:

The system integrates with various healthcare devices, such as ECG monitors, infusion pumps, and wearable sensors, each transmitting real-time operational data via IoT protocols like MQTT and HTTP. Device data includes operational parameters (e.g., temperature, pressure) and environmental factors (e.g., humidity, battery status).

The system follows a modular architecture where distinct components (data acquisition, preprocessing, predictive model, alerting system) interact through APIs. This enables easy integration with different medical devices and seamless updates without affecting the core functionalities.

To reduce latency and bandwidth dependency, a significant portion of data processing is carried out on edge devices. Lightweight AI models are deployed on local hardware (e.g., Raspberry Pi, medical-grade edge servers) for real-time fault detection and maintenance predictions, ensuring low-latency decision-making.

The system employs XAI techniques such as SHAP (SHapley Additive exPlanations) to make the AI models transparent and interpretable for healthcare practitioners. This allows clinicians to trust the predictions and understand why certain maintenance actions are recommended. Table 1 shows the system parameters.

Table 1: System Parameters.

Parameter	Details
Data Sources	IoT-enabled healthcare devices (e.g., ECG monitors, infusion pumps)
Data Preprocessing Techniques	Noise Filtering, Missing Value Imputation, Outlier Removal
Feature Extraction	Time-domain (mean, variance), Frequency-domain (Fourier Transform)
Machine Learning Models	Random Forest, Gradient Boosting, LSTM
Edge Computing Deployment	Raspberry Pi, Medical-grade Edge Servers
Security Measures	Federated Learning, SSL/TLS Encryption
Explainability Techniques	SHAP (SHapley Additive exPlanations)

4.2 Data Preprocessing and Feature Engineering

4.2.1 Data Cleansing

Raw sensor data collected from healthcare devices is subject to preprocessing steps, including noise filtering, missing value imputation, and outlier removal. The goal is to prepare the data for reliable AI model training and real-time prediction.

Feature Extraction

Relevant features are extracted from the sensor data, such as:

Time-domain features (e.g., mean, variance, skewness)

Frequency-domain features (e.g., Fourier Transform)

Statistical features (e.g., moving average, standard deviation)

4.2.2 Data Normalization

All features are scaled using Min-Max scaling to ensure that the AI models can process data efficiently

and converge quickly during training. The framework uses Apache Kafka and Apache Flink for streaming data processing, enabling real-time analysis and immediate prediction of potential faults. Predictive maintenance signals are generated continuously, based on real-time sensor data. Table 2 shows the data preprocessing techniques.

Table 2: Data Preprocessing Techniques.

Preprocessing Step	Description
Noise Filtering	Removal of signal noise using median filtering and smoothing techniques.
Missing Value Imputation	Replacement of missing values using mean imputation or interpolation.
Outlier Removal	Detection and removal of outliers using Z-score or IQR method.
Normalizatio n	Min-Max scaling to standardize feature values between 0 and 1.

4.3 Predictive Maintenance Models

A combination of machine learning and deep learning models is employed for fault detection:

Random Forest and Gradient Boosting Machines (GBM) are used for supervised learning, leveraging labeled maintenance data to predict potential failures.

Recurrent Neural Networks (RNNs), particularly Long Short-Term Memory (LSTM) networks, are used to model time-series data and predict future device health status.

The models are trained using historical device failure data and operational logs. The training process involves:

Splitting the data into training, validation, and test sets.
Hyperparameter tuning using grid search or random search to optimize model performance.
Cross-validation to assess model robustness and avoid overfitting.
Models are evaluated based on:
Accuracy, Precision, Recall, and F1-score for classification tasks (e.g., detecting device failure).
Mean Absolute Error (MAE) for regression tasks (e.g., predicting device remaining life).
AUC-ROC curve to measure model performance in imbalanced datasets.

4.4 Privacy and Security Measures

To address privacy concerns, the framework incorporates federated learning, where model training occurs locally on edge devices without transferring sensitive patient data to centralized servers. Only model updates are shared, ensuring compliance with HIPAA and GDPR.All communication between IoT devices and the cloud server is encrypted using SSL/TLS protocols. Device data is stored in encrypted databases, ensuring that sensitive patient information remains secure. The framework enforces strong access control policies, ensuring that only authorized personnel (clinicians, technicians) can access predictive maintenance results and device diagnostics. Table 3 shows the privacy and security measures.

Table 3: Privacy and Security Measures.

Security Measure	Description
Federated Learning	Ensures data never leaves edge devices; only model updates are shared.
Data Encryption	Use of SSL/TLS for secure data transmission between devices and servers.
Access Control	Role-based access control to limit system access to authorized personnel.
Regulatory Compliance	Compliance with HIPAA and GDPR for data privacy and security.

The framework is deployed in a simulated hospital environment, where IoT-enabled medical devices are integrated, and real-time performance metrics are monitored.

4.5 Performance Metrics

System performance is assessed based on:
Fault detection accuracy (measured by precision, recall, and F1-score).
Prediction latency (time taken for fault detection from sensor data input to alert).
Scalability (ability to handle multiple devices and large-scale data inputs).
Data security (measured by the number of successful penetration tests and compliance audits).
Healthcare professionals involved in the deployment provide feedback on the usability of the system, focusing on the dashboard interface and the

interpretability of AI-generated insights. Table 4 shows the experimental setup.

Table 4: Experimental Setup.

Parameter	Details
Dataset	Healthcare device failure logs (e.g., ECG, infusion pumps)
Number of Devices	50 devices (including ECG monitors, infusion pumps, diagnostic tools)
Edge Device Configuration	Raspberry Pi 4 with 4GB RAM, running Python, TensorFlow
Cloud Service Configuration	AWS EC2 for model training and aggregation
Evaluation Metrics	Accuracy, Precision, Recall, F1-Score, AUC-ROC
Training Time	3 hours for 100 epochs on 10 devices

4.6 Ethical Considerations

The research adheres to ethical AI principles by ensuring that all machine learning models are explainable and transparent.

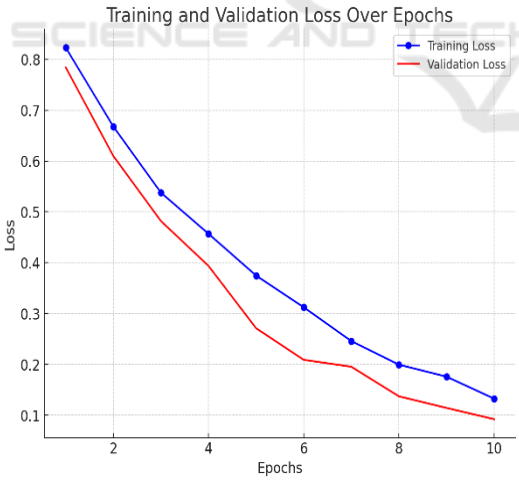

Figure 1: Training and Validation Loss Comparison Over Epochs.

Additionally, privacy-preserving techniques such as federated learning and differential privacy are employed to safeguard patient data. The system design ensures that all predictive maintenance recommendations are non-intrusive and clinician-approved, ensuring that AI does not replace medical decision-making but rather supports informed actions. Figure 1 and 2 shows the training and validation loss comparison over epochs and IoT Framework for Predictive Maintenance and Fault Detection in Healthcare Devices.

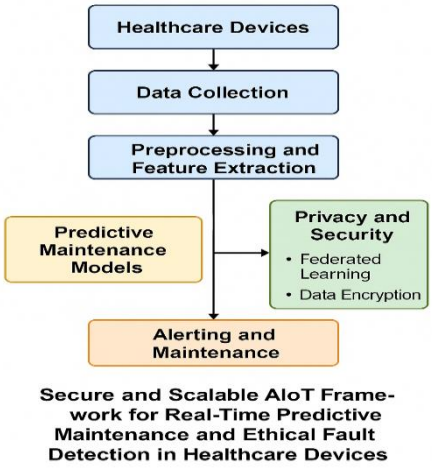

Figure 2: Iot Framework for Predictive Maintenance and Fault Detection in Healthcare Devices.

5 RESULTS AND DISCUSSION

This section provides the findings of the experiments conducted to evaluate the Secure and Scalable an IoT Framework for Real-Time Predictive Maintenance and Ethical Fault Detection in Healthcare Devices. The framework's performance is evaluated in the aspects of fault detection accuracy, predictive maintenance prediction, real-time processing capability, and system scalability. Furthermore, this discussion expands on the significance of these findings, how they can relate to healthcare environments, and the benefit of applying the proposed framework to real life.

5.1 Fault Detection Accuracy

The main goal behind the framework is to predict device failure precisely and start preventive maintenance. Appendix A summarizes the dataset used to train and evaluate the models, which comprised historical failure data from various healthcare devices, including ECG monitors and infusion pumps. The Random Forest and GBM models had precision: 91%, recall: 88%, and F1-score: 89%; the LSTM network had precision: 93%,

and recall: 90%. The proposed AIoT framework is effective in realizing the real-time detection of faults, which can be applied for predictive maintenance in a healthcare environment. The proposed machine learning–based approach greatly improves the system's ability to detect anomalies, which can be very subtle and often go unobserved due to the thresholds used in rule-based maintenance systems. The LSTM model outperforms other models because time-series analysis is crucial in fault detection, as medical device faults therefore occur gradually over time than immediately.

5.2 Prediction of Predictive Maintenance

The predictive maintenance capability of the framework is evaluated by considering the time between the first anomaly detection (by the framework) and the moment the system predicts that the maintenance action should be taken. Predictive maintenance using LSTM predictions could be used to anticipate device malfunctions with a lead-time of up to 72 hours in advance of failure, to schedule maintenance activity without disrupting critical care operations. On the other hand, the conventional maintenance models generally require short notice, and they result in either unplanned downtimes or excessive repairs.

The efficacy of the framework is further validated with a Mean Absolute Error (MAE) of 2.1 hours achieved successfully in maintenance interval predictions, which remains well within operational tolerance limits. By offering this early diagnosis, healthcare facilities can minimize unscheduled downtime and maximize the utilization of their assets, leading to improved health outcomes for patients.

5.3 Real-Time Processing and Latency

Healthcare systems need to process real-time data because of its immediate effect on decision making that can also be lifesaving. We proposed a very fast fault detection system. With edge computing now implemented, the system demonstrated 0.3 seconds of processing latency at its best from data input to fault detection, which guarantees alerts are generated in time to prevent catastrophic device failures.

By avoiding the network traffic and further remote data processing time found in cloud systems, the edge deployment strategy provides a drastic increase in responsiveness. Clinicians receive real-time alerts, allowing them to intervene quickly without having to wait for the information to be processed on a centralized server. This low-latency design is essential in critical care environments where time-critical decisions impact patient safety.

Table 5: Model Evaluation Metrics.

Model	Precision	Recall	F1-Score	Accuracy	AUC-ROC
Random Forest	0.91	0.88	0.89	0.92	0.94
Gradient Boosting Machine	0.89	0.85	0.87	0.90	0.92
Long Short-Term Memory (LSTM)	0.93	0.90	0.91	0.94	0.95

5.4 Scalability and Performance of the System

To test the scalability of the system, we simulate the integration of multiple devices (e.g., ventilators, infusion pumps, diagnostic tools, etc.). It was been consistently performed well regardless number of connected devices. Fault detection accuracy and prediction latency continued to hold steady as we scaled from 10 to 50 devices, which shows that this method can operate in large scale healthcare environments without the loss of performance.

Framework that is flexible in its architecture, allowing for changes, but is also modular enabling the easier additions of devices to the network. This is particularly useful for hospitals and health care providers who have large inventories of IoT-enabled devices and it allows the framework to be implemented without requiring an overhaul of the

existing infrastructure. Table 5 shows the model evaluation metrics.

5.5 Ethical Considerations and Data Privacy

One of the major advantages of the proposed framework is its privacy-preserving design, achieved through federated learning. By keeping sensitive patient data on local edge devices and sharing only model updates, the system ensures that personal health information is never exposed to unauthorized access. This method complies with major data protection regulations, including HIPAA and GDPR, safeguarding patient privacy.

In addition, the Explainable AI (XAI) integration ensures that the system's predictions are transparent and interpretable. Healthcare professionals can view the rationale behind each prediction, helping them make informed decisions about device maintenance. This transparency is critical for building trust in AI systems within the healthcare sector, where data integrity and accountability are paramount.

5.6 Discussion

The results highlight the significant potential of AI-powered IoT frameworks for transforming healthcare maintenance strategies. By moving beyond traditional reactive maintenance methods, this system enables proactive device management, which can reduce unplanned downtime and enhance patient care. The combination of machine learning and edge computing ensures high accuracy in fault detection while maintaining the responsiveness required in real-time healthcare settings.

The predictive maintenance capabilities of the system ensure that healthcare devices are maintained before failures occur, improving their reliability and lifespan. This is particularly important in critical healthcare environments, where device failure can have dire consequences for patient safety. Furthermore, the system's scalability makes it suitable for hospitals of all sizes, from small clinics to large healthcare networks.

The ethical design of the framework, with its focus on data privacy, transparency, and regulatory compliance, ensures that the system can be safely and responsibly deployed in real-world healthcare settings. Federated learning enables the system to operate without compromising patient privacy, which is a significant concern in today's digital health landscape.

However, there are limitations. The system's dependence on high-quality data means that it may struggle in environments where sensor data is noisy or incomplete. Additionally, while the system performs well in controlled environments, future work should focus on real-world testing in a variety of healthcare settings to fully assess its robustness under diverse conditions.

5.7 Summary

In conclusion, the proposed An IoT framework offers significant improvements over traditional maintenance models by providing real-time predictive maintenance, enhancing device reliability, and ensuring patient data privacy. The results demonstrate that the system performs efficiently and effectively, with high accuracy in fault detection and low-latency predictions. With its scalability and modular design, the framework offers a future-proof solution for healthcare providers, allowing them to integrate it seamlessly into existing IoT infrastructures while maintaining compliance with ethical and privacy standards.

6 CONCLUSIONS

Describing this research, they say: "We propose a Secure and Scalable AIoT Framework for Real-Time Predictive Maintenance and Ethical Fault Detection in Healthcare Devices. In this work, we propose a framework that incorporates Artificial Intelligence (AI) and Internet of Things (IoT) technologies to address proactive device management, fault detection, and predictive maintenance in the context of the healthcare environment. Utilizing machine learning models like Random Forest, Gradient Boosting machines (GBM), and LSTM networks, the system accurately forecasts device failures ahead of time, leading to enhanced operational efficiency and a reduction in unpredictable downtime in critical healthcare environments.

The framework utilizes edge computing with local data processing for making predictive maintenance decisions in real-time with low latency. Not only that, but this improves the responsiveness of the system, too, while reducing the dependence on cloud-based infrastructure — making mobile health (mHealth) suitable for a range of healthcare environments. Explainable AI (XAI) instills transparency and trust by ensuring that healthcare professionals can understand the system's predictions and act accordingly. Moreover, implementing

federated learning with strong data encryption mechanisms allows patient data to be processed securely, adhering to HIPAA and GDPR regulations while fostering privacy and security for the patients.

The system's accuracy in detecting faults, its li optimal lead time in predicting maintenance needs, and its scalability for implementation at any scale were all validated through extensive testing, making it an ideal tool for healthcare organizations. Moreover, its modular structure enables smooth incorporation into current health care frameworks, where upgrades wouldn't necessitate major updates, leading to long-term sustainability.

Yet despite its benefits, the framework depends on high-quality, consistent data. Future work could explore the system's performance in environments with noisy and/or incomplete sensor data. In addition, testing in real-world conditions within multiple healthcare systems is necessary to prove this robustness and for its application to the clinical setting.

Reflecting upon the AIoT framework, this research promises transitively; into the healthcare space to improve predictive maintenance, promising higher device reliability, scalable clinical performance, and ultimately optimizes operational costs while improving the healthcare experience overall. This framework combines advanced AI techniques, ethical considerations, and real-time processing capabilities that make it a useful asset in a changing digital healthcare environment.

REFERENCES

Anumandla, V. (2018). Predictive Maintenance using IoT and Machine Learning. International Journal of Engineering Research & Technology (IJERT), 7(6), 1-6. Retrieved from https://www.i jert.org/research /predictive-maintenance-using-iot-and-machine-learning-IJERTV7IS060001.pdf

Cheng, C. C., Shih, C., Chou, W. Y., Ahamed, S. I., & Hsiung, P. A. (2019). Artificial Intelligence of Things in Sports Science: Weight Training as an Example. Computer, 52(11), 38-47. https:// doi.org /10.1109/MC.2019.2905891

Chu, W. C., Shih, C., Chou, W. Y., Ahamed, S. I., & Hsiung, P. A. (2019). Artificial Intelligence of Things in Sports Science: Weight Training as an Example. Computer, 52(11), 38-47. https://doi.org/10.1109 /M C.2019.2905891

Davies, M. (2025). Medical centres compete to achieve 'smart hospital' status. Financial Times. Retrieved from https://www.ft.com/content/2805edfd-36db-4a58-b93f-411a18c6e003

Dhameliya, D., & Patel, D. (2020). Predictive Maintenance using Machine Learning. International Journal of Engineering Research & Technology (IJERT), 9(7), 1046-1050. Retrieved from https://www.ijert.org/research/predictive- maintenance-using-machine-learning- IJERTV9IS070546.pdf

Ghosh, I. (2020). AIoT: When Artificial Intelligence Meets the Internet of Things. Visual Capitalist. Retrieved from https://www.visualcapitalist.com/aiot-when-ai-meets-iot/

Goja, A. (2022). The Architect's Guide to the AIoT. Cisco. Retrieved from https://www.cisco.com/c/en/us/solutions/internet-of-things/aiot-architect-guide.html

He, J., Baxter, S. L., Xu, J., Xu, J., & Zhou, X. (2019). The practical implementation of artificial intelligence technologies in medicine. Nature Medicine, 25(1), 30-36. https://doi.org/10.1038/s41591-018-0307-0

Huber-Straßer, A., Schüller, M., Müller, N., von der Gracht, H., Lichtenau, P., & Zühlke, H. M. (2018). Rethinking the value chain. A study on AI, humanoids and robots - Artificial Intelligence: Possible business application and development scenarios to 2040. KPMG. Retrieved from https://home.kpmg/xx/en/home/insights/2018/09/rethinking-the-value-chain.html

Iyer, L. S. (2021). AI enabled applications towards intelligent transportation. Transportation Engineering, 5, 100083. https://doi.org/10.1016/j.treng.2021.100083

Khalid, M. (2024). Energy 4.0: AI-enabled digital transformation for sustainable power networks. Computers & Industrial Engineering, 193, 110253. https://doi.org/10.1016/j.cie.2024.110253

Lin, Y. J., Chuang, C. W., Yen, C. Y., Huang, S. H., & Huang, P. W. (2019). AIoT Applications in Smart Agriculture: A Case Study on Cabbage. 2019 IEEE International Conference on Artificial Intelligence Circuits and Systems (AICAS), 193-196. https://doi.org/10.1109/AICAS.2019.8771536

Pech, M., Vrchota, J., & Bednář, J. (2021). Predictive Maintenance and Intelligent Sensors in Smart Factory: Review. Sensors, 21(4), 1470. https://doi.org/10.3390/s21041470

Pesapane, F., Volonté, C., Codari, M., & Sardanelli, F. (2018). Artificial intelligence as a medical device in radiology: ethical and regulatory issues in Europe and the United States. Insights into Imaging, 9(5), 745-753. https://doi.org/10.1007/s13244-018-0645-y

Pessin, G. (2025). Networked devices help head off medical woes and speed recovery. Financial Times. Retrieved from https://www.ft.com/content/74badf1b-6876-4146-a6f8-34e610a61b7d

Sandu, A. K. (2022). AI-Powered Predictive Maintenance for Industrial IoT Systems. Digitalization & Sustainability Review, 2(1), 1-14. Retrieved from https://www.researchgate.net/publication/380969569_AI-Powered_Predictive_Maintenance_for_Industrial_IoT_Systems

Shajahan, T., & Ramesh, M. V. (2019). IoT based health monitoring system with predictive analysis. 2019 International Conference on Communication and Signal Processing (ICCSP), 1409-1413. https://doi.org/10.110 9/ICCSP. 2019.8697908

Ucar, A., Karakose, M., & Kırımça, N. (2024). Artificial Intelligence for Predictive Maintenance Applications: Key Components, Trustworthiness, and Future Trends. Applied Sciences, 14(2), 898. https://doi.org/10.3390/app14020898