Proceedings of the 8th IEOM Bangladesh International Conference on Industrial Engineering and Operations Management, Dhaka, Bangladesh, December 20-21, 2025

Proceedings of the International Conference on Industrial Engineering and Operations Management

Publisher: IEOM Society International, USA DOI: 10.46254/BA08.20250021
Published: December 20, 2025

Predictive Analytics in Smart Healthcare: Utilizing IoT Data and Machine Learning for Personalized Health Management

Md. Abdul Malek Sobuj, Md. Shareare Pervez Opi, Fariha Rahman, Gourab Saha, Khondoker MD Asif Zubayer and Fatema Tuz Zohra
Department of Computer Science and
Department of Mathematics
American International University-Bangladesh
Dhaka, Bangladesh
23-51821-2@student.aiub.edu, 23-51130-1@student.aiub.edu,
23-51121-1@student.aiub.edu, 23-51313-1@student.aiub.edu,
23-51038-1@student.aiub.edu,
fatema@aiub.edu

Abstract

The combination of Internet of Things (IoT) technologies and machine learning (ML) has opened new possibilities for predictive and personalized healthcare. This research explores how users perceive IoT-enabled healthcare systems, focusing on accuracy, trust, and privacy, which are critical factors for adoption. A quantitative survey involving 207 participants was carried out to analyze device usage trends, the reliability of health metrics, and how people respond behaviorally to predictive feedback. The findings reveal that while participants showed considerable confidence in metrics like heart rate and physical activity, they were more doubtful about advanced measurements such as blood pressure and electrocardiogram (ECG) monitoring. Privacy and data security were identified as the most important factors influencing trust, followed by the importance of medical validation and clarity in predictive results. Furthermore, insights from IoT devices were found to positively affect preventive health behaviors, including a rise in physical activity, dietary changes, and more frequent medical consultations. To address these insights, this paper suggests a framework that prioritizes trust, protects privacy, and adapts behavior, integrating explainable artificial intelligence (XAI), federated learning, and adaptive feedback mechanisms. By aligning technical precision with user-focused needs, the framework lays the groundwork for creating scalable, transparent, and secure predictive healthcare solutions.

Keywords
IoT, machine learning, predictive analytics, healthcare and user trust.

1. Introduction
The convergence of Internet of Things (IoT) technologies and machine learning (ML) is transforming healthcare by shifting from reactive treatment to a focus on personalized and preventive care. Devices like smartwatches, fitness trackers, and connected medical sensors continuously monitor health indicators such as heart rate, blood pressure, physical activity, and sleep patterns. Through predictive modeling, the analysis of these data streams yields essential insights that can assist in identifying early risks and facilitating timely interventions before conditions escalate (Rahman et al., 2024). However, the broad implementation of IoT-enabled healthcare solutions is still limited. Issues regarding device accuracy, a lack of clarity in predictions, and concerns over privacy present significant challenges. Many users question the reliability of the data produced by wearables, are hesitant to trust machine learning models

that do not provide clear explanations for their forecasts and are wary of the potential misuse of sensitive health information (Li et al., 2021; Kumar et al., 2023). While existing research has mainly focused on enhancing algorithmic precision and disease prediction models, it has frequently neglected the human aspects. In particular, studies have not adequately explored how users perceive reliability, how trust affects adoption, and how privacy concerns influence their willingness to engage with IoT systems (Badawy et al., 2023; Javaid et al., 2022).

This research aims to bridge that gap by merging survey-based findings with innovative methods to balance technical efficiency and user expectations. It investigates how individuals use IoT devices, what health metrics they prioritize, and their perspectives on accuracy, trust, and privacy. Additionally, it introduces a trust-aware framework that combines explainable AI, federated learning for secure data management, and adaptive systems capable of enhancing predictions based on user input. By aligning technological innovations with user-centered design principles, this research illustrates how IoT-enabled predictive healthcare can provide dependable outcomes while building trust, thus paving the way for scalable preventive and personalized healthcare solutions.

1.1 Objectives

The objective of this study is to investigate how users perceive IoT-enabled predictive healthcare systems and to identify the factors that influence their trust, acceptance, and behavior. This research seeks to understand the perceived accuracy and reliability of commonly monitored IoT health metrics, such as heart rate, sleep patterns, blood pressure, and oxygen saturation. It also aims to explore how privacy concerns data security, transparency of predictions, and medical validation shape user trust. Additionally, the study examines how insights generated by IoT devices influence preventive health actions, including lifestyle changes and medical consultations. Based on these findings, the study aims to develop a trust-aware, privacy-preserving framework that integrates explainable AI and federated learning to enhance reliability, transparency, and user acceptance of predictive healthcare systems.

2. Literature Review

The integration of the Internet of Things (IoT) in healthcare has increased rapidly, allowing for ongoing monitoring of vital signs and the creation of extensive datasets for predictive analysis. Li et al. (2021) conducted a study on IoT-enabled healthcare systems, underscoring the support wearables provide for predicting chronic diseases. Rahman et al. (2024) pointed out that the combination of machine learning and IoT is transforming healthcare towards personalized and predictive medicine, while Rahman et al. (2023) demonstrated its contribution to enhancing patient outcomes. In a similar vein, Nancy et al. (2022) suggested an IoT-cloud system for predicting heart disease, and Charfare et al. (2025) introduced a smart healthcare framework that merges IoT with machine learning for real-time monitoring.

Machine learning is pivotal in the realm of predictive analytics. Ganesan (2020) investigated the use of deep learning in analyzing electronic health records to enhance decision support. Paul and Beulah (2024) assessed the integration of ML and IoT for precision healthcare, whereas Yigit et al. (2024) researched ML applications within healthcare management. Junaid et al. (2022) conducted a survey of emerging technologies, emphasizing the effectiveness of combining IoT and ML for more efficient health systems. These investigations confirm that predictive analytics can boost efficiency, resource utilization, and personalization.

Despite the progress made, notable challenges remain. Javaid et al. (2022) recognized ethical and technical issues such as interoperability and reliability. Karatas et al. (2022) discussed the financial and integration hurdles faced in Industry 4.0 healthcare. Kumar et al. (2023) pointed out the lack of transparency in AI models, which undermines trust. Earlier, Ahamed and Farid (2018) acknowledged the infancy of IoT-ML applications, while Badawy et al. (2023) and Rahman et al. (2024) contended that the effectiveness of predictive analytics relies on the presence of trust and transparency.
Privacy and security are critical concerns. Aldahiri et al. (2021) examined IoT-ML health prediction systems and highlighted the necessity of privacy-preserving methods for maintaining user trust. Rahman et al. (2024) also recognized transparency and acceptance as key factors that drive adoption. Sunny et al. (2024) demonstrated that secure IoT infrastructures are vital for the successful implementation of ML in healthcare. Collectively, these studies emphasize that without adequate privacy and trust measures, IoT-based healthcare systems may face rejection.

The existing literature indicates that IoT and ML have significant potential for predictive healthcare (Rahman et al., 2024; Li et al., 2021; Ganesan, 2020; Paul and Beulah, 2024). Nonetheless, most frameworks prioritize technical precision while overlooking human factors such as trust, usability, and perceived reliability (Kumar et al., 2023;

Karatas et al., 2022; Aldahiri et al., 2021). This research aims to build on previous studies by integrating user perceptions with technical advancements and suggesting a framework for IoT-based predictive healthcare that is aware of trust, preserves privacy, and adapts to user behavior.

3. Methods

This study used a quantitative survey design to assess user perceptions of IoT-enabled predictive healthcare, focusing on accuracy, trust, and privacy. The data was analyzed from 207 respondents using descriptive statistics and a Trust Index to evaluate usage patterns and adoption factors.

3.1 Study Design

This research utilized a quantitative survey-based methodology to explore users' perceptions of IoT-enabled healthcare and predictive analytics. The design aimed to gather both objective information about device utilization and health metrics, as well as subjective insights regarding accuracy, trust, and privacy issues.

3.2 Participants

A total of 207 individuals participated in the survey. The sample comprised people from diverse age ranges, genders, and professions, all of whom had experience with wearable or IoT-based healthcare devices such as smartwatches, fitness trackers, or medical sensors. Participation was voluntary, and respondents were assured that their data would be kept confidential and utilized solely for academic purposes.

3.3 Survey Instrument

The questionnaire was divided into four sections: demographics, IoT device usage, perceptions of accuracy and trust, and behavioral outcomes. Questions covered the types of devices used, the frequency of monitoring, health metrics tracked (e.g., heart rate, blood pressure, sleep, oxygen saturation), and respondents' opinions on reliability, privacy, and transparency. Additional items inquired whether insights from IoT affected preventive measures, such as modifications in exercise, diet, or medical consultations.

3.4 Data Collection

The survey was distributed electronically, utilizing digital forms to ensure ease of access and effective data collection. Respondents were able to complete the survey using mobile phones, laptops, or tablets, promoting greater accessibility. Before distribution, the questionnaire underwent pilot testing with a small group to assess its clarity and consistency, leading to minor revisions.

3.5 Data Analysis

Data from the 207 respondents were analyzed employing descriptive statistics to summarize demographic characteristics, device usage, and perceptions of accuracy. A Trust Index was created by aggregating responses related to transparency, privacy, and predictive reliability. The relationships between demographic variables and levels of trust or device usage were investigated, and the results were interpreted within the context of the proposed trust-aware, privacy-preserving framework.

4. Results and Discussion

The analysis of 207 participants offers significant insights into the utilization of IoT devices, perceived reliability of health metrics, confidence in predictive models, and the influence of IoT-enabled healthcare on behavior.

4.1 Metrics Monitored and Perceived Reliability

The health metrics most frequently monitored included heart rate (85%), steps (77%), and sleep patterns (69%), followed by blood pressure (43%) and oxygen saturation (39%), with a smaller percentage of participants using devices that track ECG/EKG (20%) (Table 1). Participants showed the greatest confidence in the accuracy of steps and heart rate, a moderate level of trust in sleep tracking, and comparatively low confidence in blood pressure and ECG readings. These findings align with previous research indicating that consumer-grade devices are effective for basic monitoring but fall short for clinical-level assessments (Ahamed and Farid, 2018).

Table 1. IoT Metrics Tracked and Perceived Accuracy

Metric	Respondents Tracking (%	Perceived Accuracy
Heart Rate	85	High
Steps	87	High
Sleep	69	Moderate
Blood Pressure	43	Low
Oxygen Saturation	39	Low
ECG/EKG	20	Low

4.2 Trust Factors

Several critical elements shaped trust in IoT-ML healthcare systems. Privacy and data security emerged as the top concerns for 76% of participants, followed by the necessity of endorsement from healthcare practitioners at 64%, and the significance of transparency in predictions at 58% (Figure 1). This suggests that even with high accuracy in predictions, users are reluctant to embrace systems lacking robust privacy measures or professional endorsement.

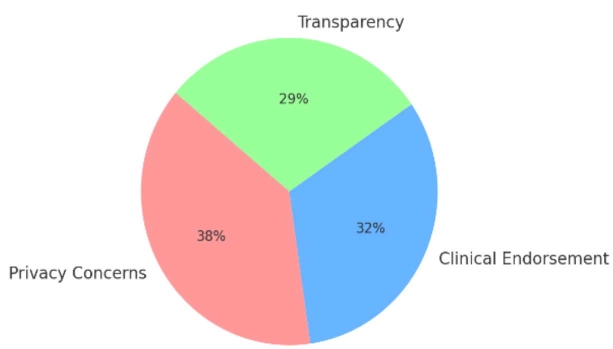

Figure 1. Trust Factors Influencing Adoption

These results align with the work of Kumar et al. (2023), who state that insufficient transparency erodes trust in AI-based healthcare, and with Aldahiri et al. (2021), who emphasize the importance of solutions that prioritize privacy.

4.3 Anticipated Predictions

Participants conveyed a strong belief that IoT-ML systems should prioritize chronic and high-burden illnesses. A significant number of anticipated predictions for heart disease (82%), followed by diabetes (69%) and mental health or stress conditions (55%) (Figure 2). Additional conditions, such as obesity, respiratory diseases, and sleep disorders also mentioned. This is consistent with prior research highlighting the promise of ML in predicting chronic diseases and facilitating preventive measures (Li et al., 2021; Nancy et al., 2022).

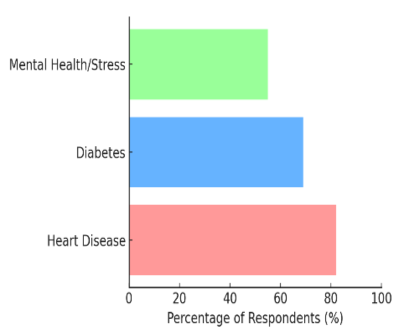

Figure 2. Predictive Expectations of IoT-ML Systems

4.4 Behavioral Responses
Insights from IoT have been shown to affect preventive health actions. Survey participants indicated that they made changes to their lifestyles based on feedback from devices, with 61% increasing their physical activity, 52% improving their diets, and 44% seeking medical advice (Figure 3). These findings underscore the behavioral influence of IoT, illustrating its capacity to promote preventive care and healthier living, which is consistent with the research by Paul and Beulah (2024) that demonstrates IoT-ML systems can inspire positive health behaviors when users trust them.

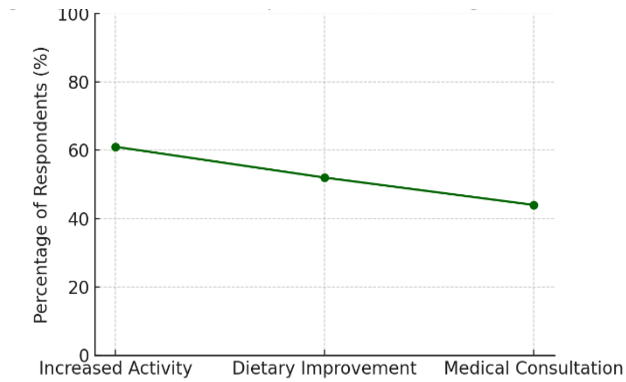

Figure 3. Behavioral Response

The study demonstrates strong involvement with basic health measures but skepticism towards more sophisticated ones like blood pressure and ECG, as reported by Ahamed and Farid (2018). Trust, particularly regarding privacy and openness, appeared as a major element in adoption, confirming Kumar et al. (2023) and Aldahiri et al. (2021). While IoT devices are intended to forecast ailments like heart disease and diabetes, insights also induced good behavior adjustments, validating Paul and Beulah's (2024) findings. These results underscore the necessity for IoT healthcare systems to balance accuracy with user confidence and privacy. The paper presents a trust-aware, privacy-preserving, and behavior-adaptive framework to overcome this gap, harmonizing with literature on transparent and secure predictive systems (Badawy et al., 2023; Junaid et al., 2022).

Some studies agree that IoT devices are reliable for basic metrics such as steps and heart rate. In contrast, other studies have shown that advanced metrics related to blood pressure and ECG have higher accuracy in more controlled or clinical settings, predominantly where the device is well-calibrated. This difference underlines that accuracy often depends on environment, device quality, and user handling. Future work should look deeper into these mixed findings.

5. Proposed Framework for Smart Healthcare
The survey findings revealed that while IoT devices are widely used for basic health monitoring, user trust remains limited due to concerns about accuracy, transparency, and privacy. These challenges highlight the need for a structured framework that not only improves technical precision but also addresses trust and user adoption barriers. To bridge this gap, the proposed Trust-Aware Predictive Framework integrates explainable AI, privacy-preserving analytics, and adaptive feedback mechanisms. Figure 4 illustrates the architecture of the proposed framework, showing how its multi-layered components work together to ensure reliability, transparency, and secure predictive healthcare delivery.

5.1 Trust-Aware Predictive Framework
To address the issue of trust in predictive healthcare, this paper presents a Trust-Aware Predictive Framework that combines explainable AI (XAI). By presenting confidence scores alongside forecasts (e.g., "elevated risk due to irregular sleep"), the system guarantees that users understand why a prediction is made, boosting transparency. This technique allows consumers to understand not just the "what" but also the "why" behind each forecast, so improving their trust in the system's reliability and accuracy.

5.2 Hybrid Accuracy-Trust Score
In classical ML models, predicted accuracy is often determined based on technical performance indicators. However, in healthcare, user perceived accuracy is just as crucial. To bridge this gap, the Hybrid Accuracy-Trust Score analyzes

both ML accuracy and user-perceived accuracy into a single composite score. This dual metric method enables continuous system improvement, guaranteeing that the model not only performs well technically but is also trusted by users, thereby promoting greater adoption.

5.3 Privacy-Preserving Predictive Analytics

A major impediment to the implementation of IoT-based predictive healthcare solutions is privacy concerns. To solve this, the proposed system mixes federated learning with edge computing. These solutions ensure that health data is processed locally on users' devices rather than being transferred to central servers, thus decreasing the danger of data breaches or misuse. By processing sensitive health data on the device, privacy is preserved, and consumers are more inclined to trust the system. Federated learning also permits model upgrades without compromising individual data privacy.

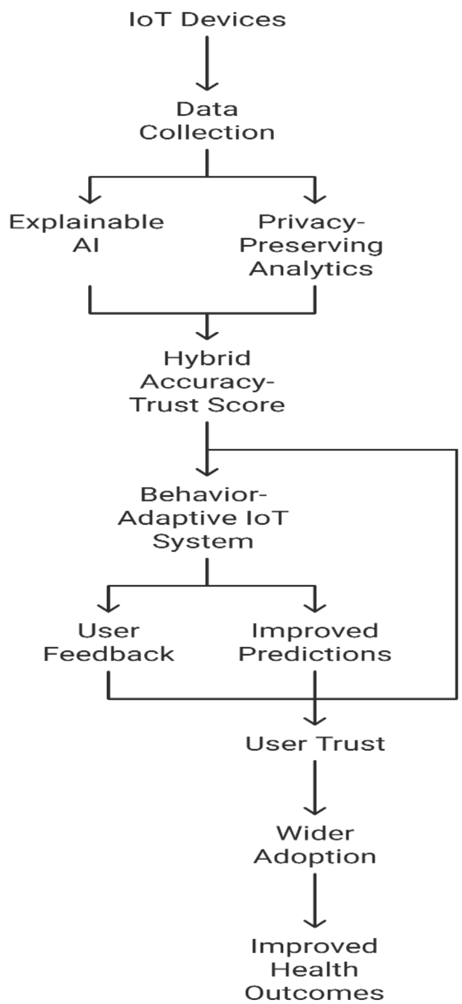

Figure 4. Trust-Aware Predictive Framework for IoT-Enabled Smart Healthcare

5.4 Behavior-Adaptive IoT System

The proposed architecture integrates a behavior-adaptive IoT system that dynamically updates predictions based on user lifestyle changes. For example, if a user follows through on IoT-based recommendations (such as altering their diet or increasing exercise), the system recalculates future risk scores accordingly. This adaptive feedback loop not only keeps predictions current but also motivates users by displaying how their actions influence results. Such tailored interaction enables continued user involvement, strengthening trust and the long-term efficiency of the system.

This multi-layered approach portrays IoT-driven predictive healthcare as not just technically robust but also trustworthy, secure, and user-centered, making it more likely to acquire wider adoption and improve health outcomes.

6. Proposed Approach

The proposed Trust-Aware Predictive Framework functions as a multi-layered system that integrates IoT-enabled data collection, privacy-preserving analytics, machine learning–based predictions, and adaptive feedback. Its workflow is illustrated in Figure 5, which depicts the architecture of the model and how each component interacts to ensure reliability, transparency, and user trust.

1. **Data Acquisition and Preprocessing:**
   Health data such as heart rate, steps, sleep duration, and blood pressure are continuously collected from IoT-enabled wearables and medical sensors. Edge computing techniques are applied to preprocess this information locally, reducing latency and minimizing privacy risks.
2. **Privacy-Preserving Analytics:**
   The framework incorporates federated learning to ensure that sensitive health data remains on user devices. Only model updates, rather than raw data, are shared across the network, significantly lowering the risk of data leakage while still improving the predictive model collaboratively.

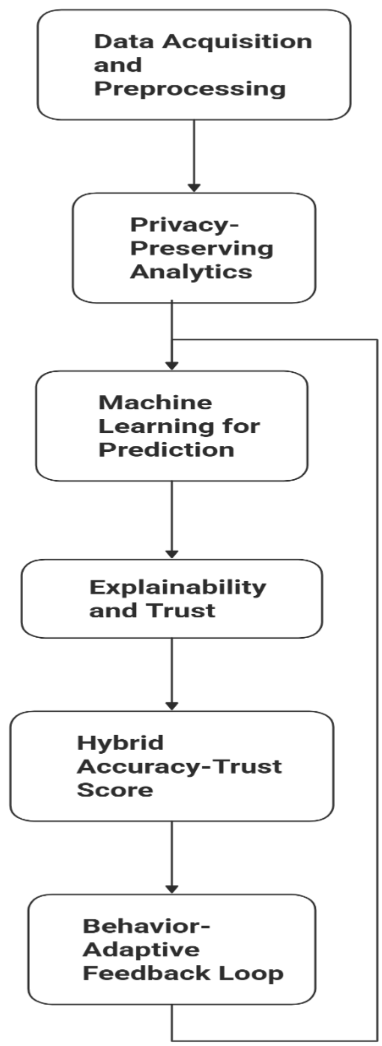

Figure 5. Workflow of the Proposed Trust-Aware Predictive System

3. **Machine Learning for Prediction:**
   Different machine learning techniques are employed depending on the nature of the data:
   Time-Series Data (e.g., ECG, heart rate, sleep patterns): Long Short-Term Memory (LSTM) networks and 1D Convolutional Neural Networks (CNNs) are used to capture sequential dependencies and detect irregularities.
   Structured Health Data (e.g., demographic, BMI, blood pressure trends): Ensemble methods such as Random Forests and Gradient Boosting (XGBoost, LightGBM) are applied to provide accurate and robust predictions.
   Baseline Models for Interpretability: Logistic Regression and Decision Trees are included to generate transparent, easily interpretable outputs that can be validated by healthcare practitioners.
4. **Explainability and Trust:**
   Predictions are supported by explainable AI (XAI) methods, such as SHAP and LIME, which highlight the most influential features contributing to each decision. This ensures that users and clinicians understand both the outcome and the reasoning process, strengthening confidence in the system.
5. **Hybrid Accuracy-Trust Score:**
   To balance algorithmic performance with user confidence, the system generates a Hybrid Accuracy-Trust Score that integrates technical accuracy metrics with user-perceived reliability, promoting long-term adoption.
6. **Behavior-Adaptive Feedback Loop:**
   The framework adapts dynamically to user behavior. When users act on system recommendations, such as increasing physical activity or improving diet, the predictive risk scores are recalculated to reflect these lifestyle changes. This real-time adaptability encourages sustained engagement and healthier habits.

   Through this integrated approach, the proposed system combines technical robustness with transparency and user-centered design. By addressing accuracy, trust, and privacy simultaneously, it establishes a scalable model for predictive and preventive healthcare.

Figure 5, illustrates the end-to-end process of the proposed approach, beginning with IoT-based health data collection and preprocessing, followed by federated learning–based privacy-preserving analytics, machine learning–driven predictions, explainability mechanisms, and behavior-adaptive feedback loops. The diagram highlights how technical accuracy, user trust, and privacy are integrated to deliver reliable predictive healthcare solutions.

7. Comparative Analysis with Existing Models

Table 2 compares the proposed trust-aware predictive framework with selected existing models. Prior studies have focused primarily on technical accuracy, such as IoT-ML disease prediction (Li et al., 2021; Rahman et al., 2023), or on real-time monitoring (Charfare et al., 2025). However, most neglected critical aspects such as user trust, privacy, and adaptive feedback. In contrast, our framework integrates explainable AI for transparency, federated learning for privacy preservation, and a behavior-adaptive feedback loop, thereby addressing both technical and human-centered requirements.

Table 2. Comparative Analysis of Existing Models and the Proposed Framework

Model	Focus	Limitation	Contribution of the paper
Li et al. (2021)	IoT + ML for chronic disease	Weak on trust & privacy	Added XAI + privacy-preserving learning
Nancy et al. (2022	IoT-cloud for heart disease	Privacy risks from centralization	Used federated + edge computing
Rahman et al. (2023/24)	Predictive analytics for outcomes	Ignored user perception	Introduced Hybrid Accuracy-Trust Score
Charfare et al. (2025)	Smart healthcare framework	Lacked structured privacy & scalability	Built behavior-adaptive + scalable design
Proposed Framework	Trust-aware IoT + ML system	Needs real-world validation	Integrates accuracy, trust, and privacy

8. Advantages of the Proposed System

The proposed Trust-Aware Predictive System offers several benefits that enhance both technical performance and user adoption:

- **Enhanced Trust and Transparency:** By integrating explainable AI and Hybrid Accuracy-Trust Scores, the system ensures that users and healthcare professionals understand how predictions are made, which fosters confidence and wider acceptance.
- **Privacy Preservation:** Through federated learning and edge computing, sensitive health data remains on user devices, significantly reducing risks of data leakage and misuse.
- **Improved Predictive Accuracy:** The combination of advanced models (LSTM, CNN, XGBoost) with interpretable baselines (Decision Trees, Logistic Regression) provides both robust predictions and transparency.
- **Adaptability to User Behavior:** The behavior-adaptive feedback loop recalculates predictions when users modify their lifestyle, reinforcing preventive health practices and promoting long-term engagement.
- **Scalability and Practicality:** The modular structure of the system allows integration with existing healthcare platforms and telemedicine services, making it suitable for deployment at larger scales.
- **Support for Preventive Care:** By enabling early risk detection and lifestyle-oriented feedback, the system can reduce healthcare costs and improve overall patient outcomes.

9. Limitations and Future Work

Limitations of this study include the sample size of 207 participants, which, while helpful, is not large enough to generalize to all users. It also does not analyze how age, gender, or education might impact trust, perceived accuracy, or behavior. Such factors provide a basis for how IoT healthcare systems are used and trusted. In addition, this study mainly compared the results with supportive literature, but some studies show different or better performance for advanced health metrics under controlled conditions. Future studies should validate the proposed framework with large-scale and longitudinal datasets, extend its application to mental health, and explore integration with telemedicine. Ensuring interoperability with healthcare infrastructures and compliance with ethical and regulatory standards will also be essential for wider adoption.

10. Conclusion

This research emphasizes the transformative capabilities of IoT-enabled predictive healthcare, highlighting its ability to encourage preventive care through ongoing monitoring and customized insights. The results indicate that while users have confidence in fundamental health metrics like heart rate and physical activity, there is lingering skepticism about more complex measurements such as blood pressure and ECG. Privacy, data security, and transparency were identified as the key factors impacting adoption, suggesting that technological precision alone does not suffice for establishing trust in predictive systems. To tackle these issues, this paper proposed a framework that is trust-aware, privacy-preserving, and behavior-adaptive, incorporating explainable AI, federated learning, and adaptive feedback mechanisms. By aligning technological advancements with the needs of the users, the suggested framework not only improves predictive accuracy but also enhances user trust, setting the stage for scalable, secure, and transparent smart healthcare solutions.

Acknowledgements

The authors would like to express their gratitude to American International University–Bangladesh for providing financial and technical support to carry out this research.

References

Rahman, M. H., Islam, T., Hossen, M. E., Chowdhury, M. E., Hayat, R., Shovon, M. S. S., and Sunny, A. R., *"Machine Learning in Healthcare: From Diagnostics to Personalized Medicine and Predictive Analytics"*, *Integrative Biomedical Research*, vol. 8, no. 12, pp. 1-8, 2024.

Li, W., Chai, Y., Khan, F., Jan, S. R. U., Verma, S., Menon, V. G., and Li, X., *"A comprehensive survey on machine learning-based big data analytics for IoT-enabled smart healthcare system"*, *Mobile Networks and Applications*, vol. 26, no. 1, pp. 234-252, 2021.

Ahamed, F., and Farid, F., *"Applying internet of things and machine-learning for personalized healthcare: Issues and challenges"*, *Proceedings of the International Conference on Machine Learning and Data Engineering (iCMLDE)*, pp. 19-21, 2018.

Yigit, Y., Duran, K., Moradpoor, N., Maglaras, L., Van Huynh, N., and Canberk, B., *"Machine learning for smart healthcare management using IoT"*, in *IoT and ML for Information Management: A Smart Healthcare Perspective*, Singapore: Springer, pp. 135-166, 2024.

Ganesan, T., *"Deep learning and predictive analytics for personalized healthcare: unlocking EHR insights for patient-centric decision support and resource optimization"*, *International Journal of HRM and Organizational Behavior*, vol. 8, no. 3, pp. 127-142, 2020.

Paul, S., and Beulah Christalin Latha, C., *"Machine Learning and IoT in Precision Healthcare"*, in *IoT and ML for Information Management: A Smart Healthcare Perspective*, Singapore: Springer, pp. 201-234, 2024.

Nancy, A. A., Ravindran, D., Raj Vincent, P. D., Srinivasan, K., and Gutierrez Reina, D., *"IoT-cloud-based smart healthcare monitoring system for heart disease prediction via deep learning"*, *Electronics*, vol. 11, no. 15, p. 2292, 2022.

Badawy, M., Ramadan, N., and Hefny, H. A., *"Healthcare predictive analytics using machine learning and deep learning techniques: a survey"*, *Journal of Electrical Systems and Information Technology*, vol. 10, no. 1, p. 40, 2023.

Javaid, M., Haleem, A., Singh, R. P., Suman, R., and Rab, S., *"Significance of machine learning in healthcare: Features, pillars and applications"*, *International Journal of Intelligent Networks*, vol. 3, pp. 58-73, 2022.

Junaid, S. B., Imam, A. A., Balogun, A. O., De Silva, L. C., Surakat, Y. A., Kumar, G., and Mahamad, S., *"Recent advancements in emerging technologies for healthcare management systems: a survey"*, *Healthcare*, vol. 10, no. 10, p. 1940, 2022.

Rahman, A., Debnath, T., Kundu, D., Khan, M. S. I., Aishi, A. A., Sazzad, S., and Band, S. S., *"Machine learning and deep learning-based approach in smart healthcare: Recent advances, applications, challenges and opportunities"*, *AIMS Public Health*, vol. 11, no. 1, pp. 58, 2024.

Karatas, M., Eriskin, L., Deveci, M., Pamucar, D., and Garg, H., *"Big Data for Healthcare Industry 4.0: Applications, challenges and future perspectives"*, *Expert Systems with Applications*, vol. 200, p. 116912, 2022.

Kumar, P., Chauhan, S., and Awasthi, L. K., *"Artificial intelligence in healthcare: review, ethics, trust challenges & future research directions"*, *Engineering Applications of Artificial Intelligence*, vol. 120, p. 105894, 2023.

Charfare, R. H., Desai, A. U., Keni, N. N., Nambiar, A. S., and Cherian, M. M., *"Smart Healthcare Framework: Real-Time Vital Monitoring and Personalized Diet and Fitness Recommendations Using IoT and Machine Learning"*, *International Journal of Robotics & Control Systems*, vol. 5, no. 2, 2025.

Rahman, A., Karmakar, M., and Debnath, P., *"Predictive analytics for healthcare: Improving patient outcomes in the US through Machine Learning"*, *Revista de Inteligencia Artificial en Medicina*, vol. 14, no. 1, pp. 595-624, 2023.

Aldahiri, A., Alrashed, B., and Hussain, W., *"Trends in using IoT with machine learning in health prediction system"*, *Forecasting*, vol. 3, no. 1, pp. 181-206, 2021.

Biographies

Md. Abdul Malek Sobuj was born in Sirajganj, Bangladesh. He is currently pursuing a Bachelor of Science degree in computer science and engineering at the American International University-Bangladesh, Dhaka, Bangladesh. His major field of study is computer science and engineering. He is eager to learn and listen. He has previously worked on academic projects in circuit design, software development, and management systems. And his research interest on Artificial Intelligence (AI), Internet of Things (IoT), Blockchain Technology, Cryptography, Quantum Computing, Machine Learning, Renewable Energy and Algorithms. He has a passion for using innovative technologies to realize practical problems and sustainable development.
Contact: 23-51821-2@student.aiub.edu

Md. Shareare Pervez Opi is an undergraduate student pursuing his Bachelor of Science in Computer Science and Engineering at the American International University–Bangladesh (AIUB). He is deeply passionate about emerging technologies and modern computing infrastructures. His research interests include Blockchain Technology, Cryptography, Cryptocurrency Systems, Cloud Computing, Containerization, and DevOps engineering. Opi is enthusiastic about exploring secure, scalable, and distributed computing models, with a strong focus on practical implementation and problem-solving. He aims to contribute to the advancement of secure digital ecosystems and automated development pipelines through innovative research and technical excellence.
Contact: 23-51130-1@student.aiub.edu

Fariha Rahman is an aspiring computer scientist currently enrolled in the Bachelor of Science in Computer Science and Engineering program at the American International University–Bangladesh (AIUB). She possesses strong

mathematical abilities, which significantly enhance her analytical thinking and research capability. Her academic and research interests include Artificial Intelligence (AI), Machine Learning (ML), and Data Science. Fariha is passionate about exploring intelligent systems, data-driven technologies, and advanced computational models. She aims to pursue higher studies in these fields to contribute to innovative research and impactful technological solutions.
Contact: 23-51121-1@student.aiub.edu

Gourab Saha is currently pursuing his Bachelor's degree in Computer Science at the American International University–Bangladesh (AIUB). His academic interests include software engineering, artificial intelligence, and the development of intelligent automated systems. He has engaged in research-oriented coursework and exploratory projects focused on AI-based system design, machine learning applications, and computational problem-solving. His current research work involves studying approaches for building efficient and reliable AI-driven solutions. Mr. Saha aims to continue developing his expertise in intelligent systems and contribute to future research in advanced software and AI technologies.
Contact: 23-51313-1@student.aiub.edu

Khondoker MD Asif Jubayer is currently pursuing his Bachelor of Science in Computer Science and Engineering (CSE) at the American International University-Bangladesh (AIUB). Driven by an inherent curiosity, he is focused on leveraging the power of coding to solve real-world challenges and develop impactful solutions. Khondoker maintains a keen interest in the rapidly evolving field of data science, aiming to translate complex datasets into actionable insights as he continues his academic and professional journey.
Contact: 23-51038-1@student.aiub.edu

Dr. Fatema Tuz Zohra, was born in 1984 in Bangladesh. I have completed my Ph.D from "Universiti Sains Malaysia" on Numerical Analysis in 2020, B.Sc. and M.Sc. in Mathematics from "University of Dhaka" in 2007 and 2009 respectively, H.S.C. from "Viquarunnisa Noon College" in 2001 and S.S.C. from "Udayan Bidyalaya" in 1999. I have started my professional career as a lecturer of Mathematics at "American International University- Bangladesh (AIUB)" in the year of 2010 and currently working as an Associate Professor of Mathematics at the same University. Interested research area of mine includes the Lie group, Lie algebra , heat, mass and microorganism transfer and Nanobioconvection.
Contact: fatema@aiub.edu