Anomaly Detection in Medical IoT devices using Federated Learning

Namratha M, Dr. Rajeshwar B S, Pooja Srinivasan, Anusree K Manoj, Niha

Department of computer Science & Engineering, B.M.S. College of Engineering, Bengaluru-560019

Abstract

The Internet of Things (IoT) is a network of physical items that are provided with the software, sensors, processing power, and other technologies and may communicate with other systems and devices over communication systems like the Internet. This work is mainly focused on the Internet of Medical Things (IoMT) which specifically focuses on healthcare and medical applications that consist of medical IoT devices. Data points or observations that diverge from the dataset's typical behavioral patterns are known as anomalies. Anomaly detection plays a prominent role in healthcare analytics as it can greatly alter the course of treatment and hence must be dealt with utmost importance. Many techniques to detect anomalies in Medical IoT devices are explored, including using conventional Machine Learning (ML) techniques. Many of these techniques are associated with centralized servers for training the data and may cause privacy issues regarding the sharing of patient information. Hence a distributed Machine learning technique, Federated learning which involves local training on decentralized edge devices and then aggregating the results on a central model thus preserving the users' privacy is explored. A system containing two IoT sensors for the measurement of pulse rate and body temperature respectively where real-time monitoring is provided through the mobile application is proposed. Federated Learning is used to implement anomaly detection and real-time feedback is provided through the application.

Keywords —*IoT, IoMT, Anomaly Detection, Federated Learning, Machine Learning*

INTRODUCTION

IoMT, also known as the Internet of Medical Things in healthcare, is a connection of hardware infrastructure, medical equipment, and software applications over the Internet. It allows secure connection of different medical devices over the Internet and facilitates quick and adaptable processing of medical data. It paves way for remote continuous real-time monitoring of patient's health and plays a crucial role within the healthcare industry to increase the accuracy, reliability, and productivity of electronic devices **(Joyia et al. 2017)**[1].IoMT needs a far more robust security infrastructure than other IoT systems need since healthcare data is so sensitive and regulated.

In the realm of health care, variables like accuracy, precision, and quality can be used to create a diagnosis and treatment plan. No device made by humans is 100% accurate hence a proper error detection mechanism needs to be in place. In the healthcare sector, an anomaly(error) can have catastrophic effects. Anomalies are data points that are distinct from the rest of the dataset and contradict the data's usual behavior. Anomalies in medical equipment can result in false results, which can lead to faulty inference and, ultimately, the wrong course of treatment. Hence anomaly detection is of the utmost importance in this field.

Anomaly detection in IoT devices in general is primarily carried out by analyzing data which is generated in vast quantities by these devices. Conventional Machine Learning algorithms draw insights from these large amounts of data by identifying patterns in them and thus can be used for analytical purposes, numerous applications combine IoT and Machine Learning including anomaly detection. But this requires large data to be shared on a central model for training purposes. This may cause privacy issues since the data produced by medical devices contain sensitive patient data. Moreover, handling huge amounts of data through wireless networks in IoMT might not be feasible.

This issue of privacy can be solved by the use of a distributed machine learning technique, Federated Learning (FL). It allows different servers or edge devices to develop and implement a shared model for training their data without the exchange of data. This ensures that the data generated by edge devices of IoMT setup are trained locally on the device and only the results obtained are shared across the system. This not only helps in maintaining privacy but also thrives

in low-latency network connections with improved learning capabilities. Hence different applications of FL, especially in the healthcare sector, are explored in this work and a system for medical anomaly detection using FL is proposed.

LITERATURE SURVEY

When handled on a big scale, conventional sensor-based diagnosis in the medical industry needs additional sensors and labor from humans. Due to the lack of medical personnel and the way the system is set up, it is a challenging endeavor. A web and mobile application based on continuous wireless patient monitoring in a low-cost system and transmitting the patient vital signs in emergencies is employed as an IoT-based healthcare application to address this issue. **(Yeri(2020))**[9].

There are different types of sensors to measure different physiological parameters. The most essential ones are heart rate and temperature which are used commonly. According to a work by **(Thomas et al. 2016)**[2], the heart rate can be measured using a heart rate sensor and temperature using an LM35 temperature sensor. This device will allow users to monitor their mean artery pressure (MAP) in under a minute and display the precise body temperature on their Android mobile. . Since these physiological factors cannot be examined by a doctor continuously, this Arduino setup aids in not only measuring but also storing data for future analysis. This also paves for remote real-time monitoring of a patient by a doctor. The data can be used to aid in the analysis and diagnosis of a condition.

Hence the accuracy of data is very important in such cases and anomalies pose a threat to the accuracy. Data points that stand out from the rest of the dataset's data points and contradict the data's usual behavior are called anomalies. These observations or data points differ from the typical behavioral patterns in the dataset. Hence, they can have huge implications in the healthcare sector where they can drastically alter the course of treatment, and the condition of the patient.

To prevent sickness from going unnoticed**, (Pachauri et.al 2015)**[3] claimed that the fundamental issue of anomaly detection in medical applications is to lower the false negative rate (FNR). But altering the algorithm to reduce FN will inevitably increase the false positive rate (FPR). Medical professionals would disregard the majority of the alarms because they would become "alarm

fatigued" from too many false positives. These occurrences would ultimately prove lethal**.** Hence anomaly detection in the healthcare sector is a very important task.

The availability of big data has paved the way for the extensive use of Deep Learning in the medical field**.(Fernando et al. 2022)**[4] published a survey on Deep Learning for medical anomaly detection, where they discuss extensively the various Deep Learning approaches used to detect outliers/abnormalities in the medical sector. It focuses on both supervised and unsupervised learning techniques. Unsupervised anomaly detection does not require the data to be labeled as normal or abnormal during its training. It uses two typical algorithms like Auto Encoders (AEs) and Generative Adversarial Networks (GANs) which use automatic feature learning to do the classification. A supervised signal is produced in the case of supervised anomaly detection, which indicates the examples which are anomalous and which are normal. Since both of these limit data transmission in one direction, Recurrent Neural Networks (RNN) were explored as a way to address this. The most common RNN types, such as Gated Recurrent Units (GRUs), Neural Memory Networks (NMNs), and Long Short-Term Memory (LSTM) Networks were reviewed. It was observed that some of these techniques were computationally expensive and hence hinders their use in lightweight IoMT systems having WSN. Lack of Generalization in data was also a key drawback which is a direct consequence of data scarcity in the medical field which is often associated with the strict regulation regarding the conduction of studies on humans and the handling of sensitive data associated with that.

Medical data also tend to have an imbalance since normal samples are more in number compared to anomalous ones. Hence an unsupervised anomaly detection algorithm introduced by **John Sipple [10**] can be used to detect device failure in IoT. They train classifiers to discriminate between positive and negative samples by creating negative samples from positive observed samples. The concentration phenomenon has been used to discover anomalies by combining negative sampling with classifiers, as well as the usage of integrated gradients, which can allot precise values to anomalies even when the state vectors are high-dimensional. This research also looked at the use of Negative Sampling Neural Network (NSNN) and Negative Sampling Random Forest (NS-RF), two negative sampling classifiers based on neural networks and random forests, respectively. But this research mainly focuses on a generalized application of IoT and a proposal

is made for a very large-scale integration with power devices. Hence this involves the complete sharing of data between the devices for augmentation and training which is not feasible for application in the Healthcare sector due to privacy regulations.

One of the most prominent reasons for the occurrence of anomalies in IOT-based health monitoring is the use of WSN(wireless sensor networks). For sensor nodes in a WSN with limited resources, traditional security strategies with substantial overhead are not practical. The use of conventional computer security approaches in a WSN is significantly hampered by a lack of data storage and power. In light of this, WSNs are susceptible to several dangers that could destroy the node and result in inaccurate data **(Jain 2011)[**5]. The detection of such anomalous data is very important to reduce false alarms.

IoT systems using WSN have limited computational power and energy resources. Additionally, their measures are vulnerable to several irregularities from incorrect calibration, electromagnetic interference, etc. To mitigate this issue,**(Pachauri et.al 2015)**[3] proposed the classification of readings as normal or abnormal using Machine Learning algorithms like K-nearest neighbor, J48 algorithms. Regression algorithms like linear regression and Additive regression were used on abnormal records to help differentiate between faulty readings and actual critical state. This was successful in detecting anomalies but had a high computational complexity. It also used a centralized server for the training of data which requires sharing of sensitive information about the patient which may hinder their privacy.

One of the main characteristics of a WSN node is the low computational complexity which hinders the use of complex Machine Learning algorithms. Hence **(Poornima et.al 2020)** [6] proposed an Online Locally Weighted Projection Regression (OLWPR) for anomaly detection in WSN. Linear Weighted Projection Regression methods are non-parametric and the predictions were performed by local functions that use only the subset of data. This ensured low computational complexity which facilitated the storage of training data locally in the nodes. However, this still doesn't guarantee a generalized fit as it's restricted to Regression. An implementation of a different Machine Learning Technique may be required which is not possible in the proposed system.

Any vulnerability in the IoT devices used in an organization opens a door for an attack which could lead to the loss of sensitive and confidential information. The majority of the studies discussed above have used conventional Machine Learning classifiers like Decision Trees (DT), Random forests (RF), Support Vector Machines (SVM), and Artificial Neural Networks (ANN) to detect anomalies in the IoT system. But most of them rely on models trained on a central dataset. This compromises the privacy of patient data in a real-time environment with a constant flow of data. Hence a distributed Machine learning technique, Federated Learning is explored by **(Wang et al. 2022)**[7] for IOT-based applications. It uses the Federated Learning approach which involves the use of a Deep Reinforcement Learning algorithm and training it locally and aggregating the results. By this method, since the model is trained locally on the datasets, the data privacy is preserved along with the assurance of low computational complexity.

(Mohammed Aledhari et al,**2020)**[11] provided a detailed overview of Federated Learning(FL) in their work which included descriptions of supporting technologies and recent research in FL. Diverse Federated Learning architectures were discussed, including horizontal, vertical, and different frameworks such as Tensorflow Federated (TFF), PySyft, Fate, and others. Many of its applications in Medical Imaging and Anomaly Detection were also studied in this research, including Google keyboard query recommendations, mobile keyboard suggestions, rating browser history suggestions, and patient clustering to predict mortality and hospital stay.

(Nguyen et.al 2021)[12] conducted a comprehensive survey regarding the use of FL in diverse IoT applications. They elaborate on different characteristics of FL like its innovative operational concept, which can offer various important benefits for IoT applications as follows:

- Privacy Enhancement: In FL, the training at the aggregator does not require the raw data. As a result, there is a reduced risk of sensitive user information being disclosed to an outside entity, and some level of data privacy is offered.
- Enhanced learning quality: FL ensures better accuracy and enhanced scalability as it pools numerous processing resources and diversified datasets because of its distributed learning nature.

- Low-latency Network Communication: As no data is transmitted between IoT devices and the server, communication latencies due to data offloading will be reduced. In addition, it also preserves network resources for data training, such as spectrum, and transmits power.

Federated Learning offers a lot of advantages over conventional ML techniques, apart from being secure. It is favorable to be used in IoT systems with low bandwidth communication paths which can't handle the massive flow of data. (**Kholod et. al**,**2014)**[13]explores a lot of these advantages. It contains a detailed survey and comparison of numerous frameworks for the implementation of FL. It uses the simplicity of deployment, performance, development, accuracy, and analysis as parameters to compare them. IoT nodes with minimal computational complexity were used.

(Chamikara et al,2021)[14] proposed the DISTPAB approach to enhance the privacy of the data and distributed machine learning in distributed systems. This approach addresses the issues of high dimensional data, which can be critical in revealing hidden patterns when large amounts of data are produced by distributed devices, such as in banking and healthcare, where data from these industries may contain potentially sensitive information that could become public if not properly sanitized.

The medical field often requires access to large amounts of data to make significant reductions in their research. The diverse nature of the data is equally necessary, prompting the need for a next-generation collaborative framework for researchers throughout the world. Hence (**Guodong Long et al,2022)**[16] proposed to implement an open innovation framework in the medical industry, known as open health, with the goal of increasing healthcare organizations' creative ideas and innovative potential by establishing a next-generation collaborative framework with researchers and partners using Federated Learning. This ensured the privacy of data in healthcare informatics along with providing a system for collaboration.

Obtaining adequate data to train a model in the medical field is difficult. Sharing data for training is also challenging due to regulatory restrictions for maintaining the privacy of the patients. Hence (**Xiaoxiao Li et al**,**2020)**[17] used federated learning in Multi-site fMRI analysis which ensures the privacy of patients' data and data isolation. For privacy protection, this study used a randomized technique. In addition, they've also demonstrated that adding domain adaptability to

federated learning can help it perform better which can be achieved using approaches like a Mixture of Experts (MoE) and Adversarial Domain Alignment. This work shows how federated learning can help with data isolation and privacy concerns.

According to a survey by **(Ahmed Imteaj 2021)**[15]**,** FL has several benefits, such as data scalability and privacy, but presupposes that edge devices have advanced computational processing power. Robots and other IoT devices have minimal bandwidth, low power, limited processing capability, and limited storage. Hence The FedIoT platform was proposed, which uses the FedDetect algorithm to find anomalies in IoT devices. Therefore, in this strategy, the best aspects of both technologies—low IoT device infrastructure and high Federated Learning computational capacity—are merged. This platform has many applications in the healthcare sector.

(Zhang et al,**2021)[**18] used the FedIoT platform to propose a federated learning architecture for on-device anomaly data detection. This work used a FedDetect algorithm to detect anomalies on IoT devices. The FedDetect Learning framework uses a local adaptive optimizer and a cross-round learning rate to improve performance. The learning rate can be changed as needed. Anomalies were detected using Autoencoder. CL-Single, in which each device's detection model is trained on its dataset, CL-Combined, in which each device trains its detection model on a combined dataset, and CL-FedDect, in which the detection model is trained using federated learning with the FedDect algorithm, which includes parameters such as each model's accuracy, true positive rate, false-negative rate, and true negative rate.

Anomaly detection in real-time continuous data provided by IoT devices which have been implemented using several machine learning algorithms does not protect the confidentiality of user data. Each device can ensure privacy by training its own detection model, however, this lacks generality in the training data and so compromises the model's accuracy. IoT in healthcare should be exceedingly accurate and secure, as well as protect patients' personal information. Federated Learning could help achieve high accuracy while protecting the privacy of users' personal data. As a result, a Federated Learning-based solution for anomaly identification in medical IoT devices is proposed in this paper.

PROPOSED SOLUTION

This methodology's action helps is to notify the user any anomalies in the temperature and pulse sensors utilizing a federated learning strategy rather than centralized training data. Using federated learning, mobile devices can work together to develop a shared prediction model while still retaining all of the training data. To make this federated learning work, an IoT setup along with an android application is developed. The IoT setup mainly consists of Arduino, temperature sensors, and heart rate sensors. The Arduino board was set up with the aid of the Arduino IDE, and the system was used to continuously collect data from the sensor and store it in the Firebase database. A NoSQL database hosted in the cloud, Firebase Database synchronizes and stores data amongst users in real-time. The android application was developed to send a notification to the user based on real-time input from the user using android studio. Flask API was used to establish a connection between the model and the application. The overall flow of work is depicted in Fig. 1.

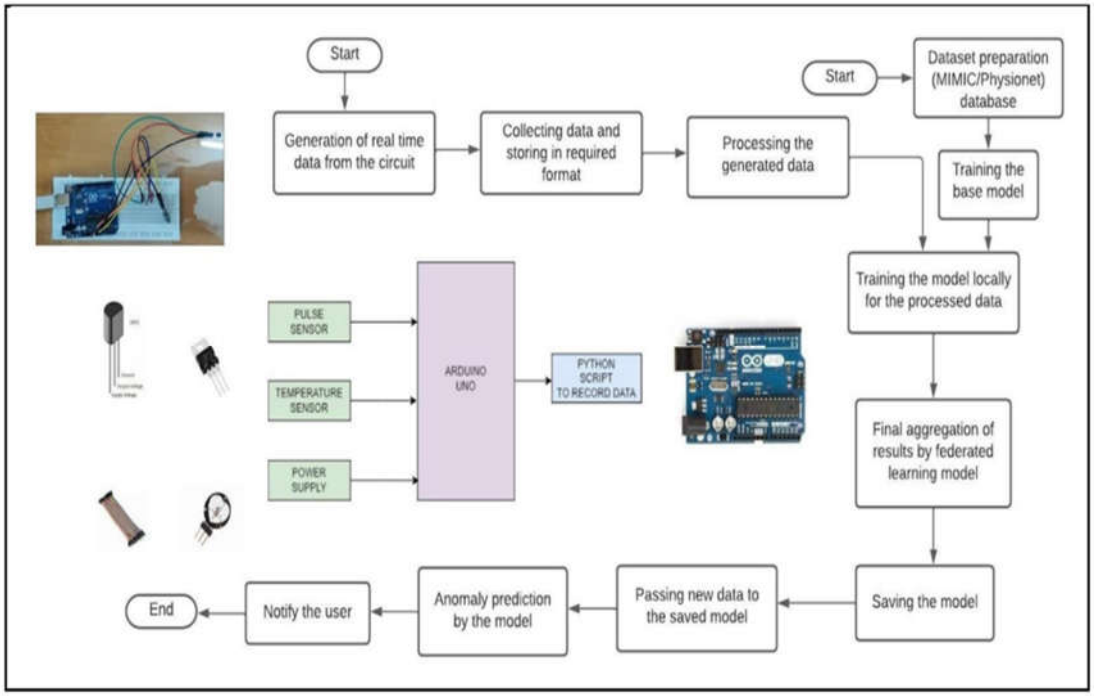

Fig 1: Proposed Solution- Design

The Internet of Things (IoT) enables data exchange between devices and systems over the Internet by connecting physical objects that are outfitted with sensors, computing power, and software. In order to detect the user's heart rate and temperature, the IoT sensor setup required attaching the

temperature sensor and heart rate sensor to the Arduino Uno board. A well-designed, low-power, plug-and-play heart-rate sensor called the Pulse Sensor for the Arduino is used to incorporate real-time heart-rate data. As blood flows through the human body, the capillary tissues' volume is impacted. The heart rate pulse sensor's LED light, which emits light after each beating, is affected by this alteration in capillary tissue capacity. Any controller can be connected to this pulse sensor in order to track the light's small variations. As a result, the LED light on each pulse sensor aids in calculating the pulse rate. By placing it in front of the pulse sensor, a human finger can be used to assess its performance. The variation in LED light acts as a barometer for the heartbeat rate of a finger. A "photoplethysmogram" is the term used to describe this phenomenon. The solid-state technique is used by the LM35 to measure temperature. The low-voltage, precise centigrade temperature sensor is the LM35. With the help of an Arduino, this chip produces a voltage that is directly proportional to the temperature in degrees Celsius. It takes use of the fact that as temperature increases, the forward voltage (Vbe), which connects the base and emitter of a diode-connected transistor, decreases steadily. It is simple to generate an analogue signal that is exactly proportional to temperature by amplifying this voltage shift in the right way. Diode-connected transistors are employed as thermometers due to the linear relationship between forward voltage and temperature.

Once the heart rate sensor and LM35 sensor were hooked up to the Arduino, the code to the Arduino was uploaded using the Arduino IDE. Arduino uses a variation of the C programming language as its programming language. A Python script was written to read the sensor value after the hardware was attached and the Arduino sketch was tested. Once the connection is established between Arduino and the python script, the python script reads data from the port. This data read is then sent to firebase using the POST API. The project utilizes a python script to send the recorded sensor data to the firebase database.

The pre-processed dataset for this work was prepared using the MIMIC dataset where more than 90 ICU patients are stored in the MIMIC Database which is further used to train the base model. The relevant parameters for this work were age, gender, weight, temperature, and heart rate and they were sorted from the MIMIC dataset by using python scripts.

The isolation forest technique, which operates on the theory that anomalies are simpler to recognize because they are made up of a small number of distinctive observations from the data,

is used to find anomalies. It is an unsupervised machine learning technique that isolates outliers from the data in order to find anomalies. It distinguishes outliers by randomly selecting a split value between the feature's maximum and minimum values by selecting a feature from a group of features. Shorter tree pathways will result from the ability to segregate the anomalous data points from the rest of the data using this random feature partitioning. The Isolation Forest separates anomalies by using an ensemble of Isolation Trees for the given data points. With Isolation Forest, this strategy discovers abnormalities more rapidly and effectively than other approaches. The isolation forest's trees can have smaller maximum depths, which minimizes the amount of memory required, because anomalous data points frequently have substantially shorter tree pathways than regular data points.

The Federated Learning approach is used for subsequent learning after the base model has been trained using the Isolation Forest technique. The client local models are then trained using the data gathered from the devices, after which the server model is updated with the base model and the clients are initially updated with the server model. All of the clients' updated training results are delivered to the server model and combined, improving the server model. The improved server model is then applied to the local models. All throughout, this procedure is continued. Data security and privacy are guaranteed by this training method, which only shares the training outcomes. The models are then examined and saved for use. An android application can deploy and test the trained model, and when an anomaly is discovered, it alerts the user. Through an application where the user's heart rate and temperature are tracked, the user can log in for a specific session. Based on the learnt model, the program alerts the user if the readings are abnormal or normal. The suggested work's system design is depicted in Fig. 2.

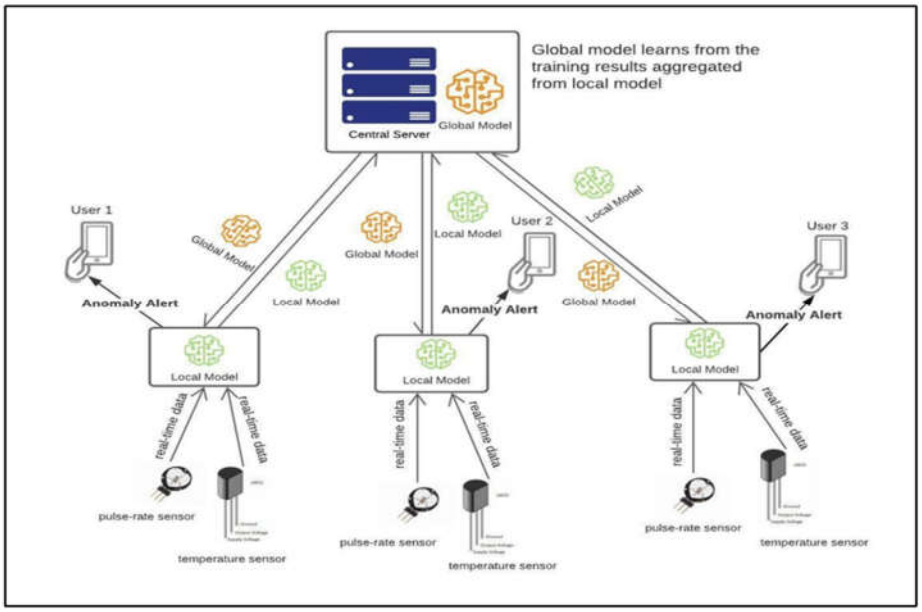

Fig 2: System Architecture

RESULTS AND DISCUSSION

An important yet difficult task is the automatic detection of irregularities in physiological data, such as temperature and heart rate readings. In fact, the level of unpredictability associated with human physiological data contributes to the difficulty in identifying anomalies in health data. The current study sheds light on the system's effectiveness in correctly spotting irregularities in the physiological data gathered. The constant training of the global model increases the system accuracy. The proposed system has been enhanced in terms of privacy and security by incorporating Federated Learning approach.

For each of the project's functional units, unit tests were written. To make the tests work, stubs were made. The main Java library utilized in this work for both unit testing and integrity testing was JUnit. Before connecting the circuits, the jumper wires' integrity and operation were checked for IoT sensors using a multimeter. Once a few modules were integrated, JUnit was utilized for integration testing in android. The final integration test was completed after all the modules had been integrated. An example sketch was executed on the Arduino IDE once the circuitry was ready for evaluating the reliability of the sensors.

The developed model successfully delivered accurate results when it was tested against the experimental dataset as shown in Fig. 3. Along with the heart rate and temperature record, the us er's weight and age groups were taken into account. The system determined whether a reading w as abnormal or normal using the readings that were logged and the fundamental trained model.

```
result.head()
```

	GENDER	ICUSTAY_ADMIT_AGE	ICUSTAY_AGE_GROUP	WEIGHT_FIRST	TEMPERATURE	HEARTRATE	clusters
4131	0.0	77	1.0	59.400000	96.099998	100.000000	0
3384	1.0	63	1.0	84.441761	97.745386	46.427333	1
71	1.0	82	1.0	55.800000	98.400002	132.000000	0
933	0.0	85	1.0	56.700000	98.000000	19.000000	1
5187	1.0	55	1.0	96.700000	96.199997	80.000000	0

Fig 3: Experimental Dataset

When the model was tested using the dataset gathered for heart rate anomaly detection, it gave results with an accuracy of 86% and a precision of 88.52%, indicating an improved quality of positive prediction. Additionally, the system is accurately recognizing the true anomalies from the dataset with a 95.14% recall value and a 91.71% F1-Score, and also indicating that there are less false alarms. The server model is updated with the testing results each time, and the client model is updated together with the server model. The model developed for heart rate detection is shown in Fig. 4.

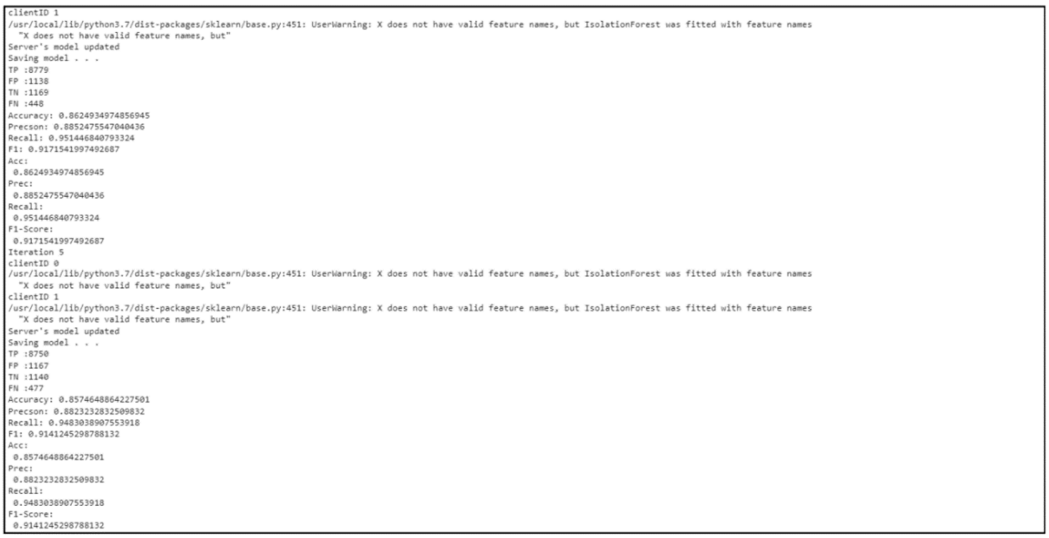

Fig 4: Model Trained for Heart Rate Anomaly Detection

The model that was trained for temperature detection is displayed in Fig. 5. The results were reliable with an accuracy of 84.23% and 83.57% precision when the model was applied to the testing dataset, indicating that the model's positive predictions were of higher quality. Additionally, the system is accurately recognizing the true abnormalities from the dataset with a 99.93% recall value and a 91.02% F1-Score, and there are less false alarms. The server model is updated with the testing results each time, and the client model is updated together with the server model.

```
clientID 1
/usr/local/lib/python3.7/dist-packages/sklearn/base.py:451: UserWarning: X does not have valid feature names, but IsolationForest was fitted with feature names
  "X does not have valid feature names, but"
Server's model updated
Saving model . . .
TP :7299
FP :1434
TN :392
FN :5
Accuracy: 0.8423877327491786
Precson: 0.8357952593610443
Recall: 0.999315443592552
F1: 0.910270000623558
Acc:
 0.8423877327491786
Prec:
 0.8357952593610443
Recall:
 0.999315443592552
F1-Score:
 0.910270000623558
Iteration 5
clientID 0
/usr/local/lib/python3.7/dist-packages/sklearn/base.py:451: UserWarning: X does not have valid feature names, but IsolationForest was fitted with feature names
  "X does not have valid feature names, but"
clientID 1
/usr/local/lib/python3.7/dist-packages/sklearn/base.py:451: UserWarning: X does not have valid feature names, but IsolationForest was fitted with feature names
  "X does not have valid feature names, but"
Server's model updated
Saving model . . .
TP :7293
FP :1440
TN :386
FN :11
Accuracy: 0.8410733844468784
Precson: 0.835108210237032
Recall: 0.9984939759036144
F1: 0.9095217309970692
Acc:
 0.8410733844468784
Prec:
 0.835108210237032
Recall:
 0.9984939759036144
F1-Score:
 0.9095217309970692
```

Fig 5: Model Trained for Temperature Anomaly Detection

The accuracy measurement of the system that was built for detecting heart rate and temperature is shown in the graph below, Fig. 6.

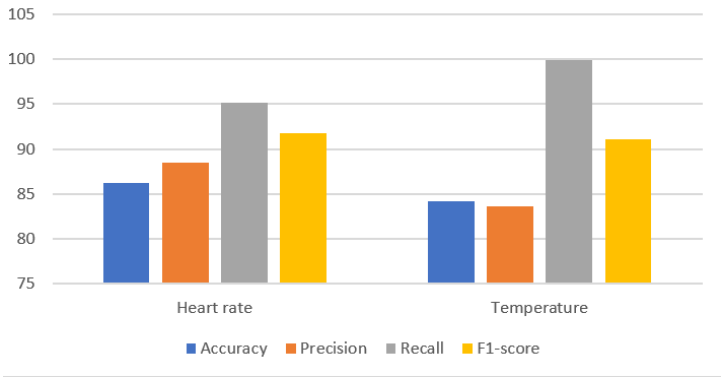

Fig 6: Bar graph depicting the accuracy of heart rate senor and temperature sensor

Clients are initially updated with the server model, and the server model is updated with the base model. The data gathered from the devices is used to train the clients' local models. The server model is improved by aggregating the updated training results from all the clients and sending them to it. The improved server model is then applied to the local models. This ongoing training procedure improves the system's accuracy.

CONCLUSION AND FUTURE ENHANCEMENTS

Real-time monitoring, robotic surgery, and other medical IoT techniques can assist patients' diseases to get better and offer a less expensive substitute for traditional medical systems. The nature of network security, however, may make it possible for anomalies to occur. On the other hand, a minor anomaly in medical IoT data can have catastrophic effects and change the course of treatment. The readings may not reveal health conditions, which could have a profound impact on people's lives. Therefore, these anomalies need to be found precisely and quickly.

The anomaly detection framework and warning system will be used to find anomalies in the users' physiological parameters, including temperature and heart rate. Any abnormalities will be immediately notified to users (i.e., patients and doctors). A real-time update on measurement changes or data abnormalities will be provided through the notification system, which will help with the ongoing examination of patients with medical problems. Accuracy and privacy are this system's two most important components. This quick and precise identification can help patients and clinicians communicate more effectively. The emerging idea of FL improves the security and handling of data to benefit many domains including the healthcare sector. FL would ensure secure data access and exchange without compromising privacy. The Federated Learning method will assist maintain the confidentiality of users' medical information while enhancing the model's precision. As it is trained locally, it may also be effortlessly incorporated into a system with high real-time data flow and low bandwidth transmission. As a result, the system guarantees user privacy, security, scalability, consistency, and excellent performance.

The proposed work uses Federated Learning to detect anomalies in two devices: heart rate and temperature sensors. This work could be expanded to include other healthcare equipment in the future such as oximeter, BP monitoring, pulse rate monitoring, or it could focus on anomaly detection relating to a specific health condition.

Conflict of Interest: The authors declare that they have no conflict of interest.

References

1. Joyia, Gulraiz J., and Rao M. Liaqat, Aftab Farooq, and Saad Rehman. 2017. “Internet of Medical Things (IOMT): Applications Benefits and Future Challenges in Healthcare Domain”. *Journal of Communications*. https://doi.org/10.12720/jcm.12.4.240-247.

2. Thomas, Salomi S., Amar Saraswat, Anurag Shashwat, and Vishal Bharti. 2016. “Sensing Heart Beat and Body Temperature Digitally Using Arduino”. In *2016 International Conference on Signal Processing Communication, Power and Embedded System (SCOPES)*. IEEE. https://doi.org/10.1109/scopes.2016.7955737.

3. Pachauri, Girik, and Sandeep Sharma. 2015. “Anomaly Detection in Medical Wireless Sensor Networks Using Machine Learning Algorithms”. *Procedia Computer Science* 70: 325–33. https://doi.org/10.1016/j.procs.2015.10.026.

4. Fernando, Tharindu, Harshala Gammulle, Simon Denman, Sridha Sridharan, and Clinton Fookes. 2022. “Deep Learning for Medical Anomaly Detection A Survey”. *ACM Computing Surveys* 54 (7): 1–37. https://doi.org/10.1145/3464423.

5. Jain, M.K. 2011. “Wireless Sensor Networks: Security Issues & Challenges,”. *IJCIT, No. 1,* 2.

6. Poornima, I. Gethzi Ahila, and B. Paramasivan. 2020. “Anomaly Detection in Wireless Sensor Network Using Machine Learning Algorithm”. *Computer Communications* 151 (February): 331–37. https://doi.org/10.1016/j.comcom.2020.01.005.

7. Wang, Xiaoding, Sahil Garg, Hui Lin, Jia Hu, Georges Kaddoum, Md. Jalil Piran, and M. Shamim Hossain. 2022. “Toward Accurate Anomaly Detection in Industrial Internet of Things Using Hierarchical Federated Learning”. *IEEE Internet of Things Journal* 9 (10): 7110–19. https://doi.org/10.1109/jiot.2021.3074382.

8. Ukil, Arijit, Soma Bandyoapdhyay, Chetanya Puri, and Arpan Pal. 2016. “IoT Healthcare Analytics: The Importance of Anomaly Detection”. In *2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)*. IEEE. https://doi.org/10.1109/aina.2016.158.

9. V. Yeri and D. C. Shubhangi, "IoT based Real Time Health Monitoring," *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, 2020, pp. 980-984, doi: 10.1109/ICIRCA48905.2020.9183194.

10. John Sipple. Interpretable, multidimensional, multimodal anomaly detection with negative sampling for detection of device failure. In International Conference onMachine Learning, pages 9016–9025. PMLR, 2020.

11. Mohammed Aledhari, Rehma Razzak, Reza M Parizi, and Fahad Saeed. Federated learning: A survey on enabling technologies, protocols, and applications. IEEE Access, 8:140699–140725, 2020.

12. Dinh C Nguyen, Ming Ding, Pubudu N Pathirana, Aruna Seneviratne, Jun Li,and H Vincent Poor. Federated learning for internet of things: A comprehensive survey. arXiv preprint arXiv:2104.07914, 2021.

13. Ivan Kholod, Evgeny Yanaki, Dmitry Fomichev, Evgeniy Shalugin, Evgenia Novikova, Evgeny Filippov, and Mats Nordlund. Open-source federated learning frameworks for iot: A comparative review and analysis. Sensors, 21(1):167,2021.

14. Mahawaga Arachchige Pathum Chamikara, Peter Bertok, Ibrahim Khalil, DongxiLiu, and Seyit Camtepe. Privacy preserving distributed machine learning with federated learning. Computer Communications, 171:112–125, 2021.

15. Ahmed Imteaj, Urmish Thakker, Shiqiang Wang, Jian Li, and M Hadi Amini. Asurvey on federated learning for resource-constrained iot devices. IEEE Internet of Things Journal, 2021.

16. Guodong Long, Tao Shen, Yue Tan, Leah Gerrard, Allison Clarke, and Jing Jiang.Federated learning for privacy-preserving open innovation future on digital health.In Humanity Driven AI, pages 113–133. Springer, 2022.

17. Xiaoxiao Li, Yufeng Gu, Nicha Dvornek, Lawrence H Staib, Pamela Ventola, andJames S Duncan. Multi-site fmri analysis using privacy-preserving federated learning and domain adaptation: Abide results. Medical Image Analysis, 65:101765,2020.

18. Tuo Zhang, Chaoyang He, Tianhao Ma, Lei Gao, Mark Ma, and Salman Avestimehr.Federated learning for internet of things: a federated learning framework for on-device anomaly data detection. arXiv preprint arXiv:2106.07976, 2021.