Online-Journals.org

iJOE International Journal of Online and Biomedical Engineering

iJOE | eISSN: 2626-8493 | Vol. 21 No. 6 (2025) | OPEN ACCESS

https://doi.org/10.3991/ijoe.v21i06.54403

PAPER

Edge Computing and Blockchain-Based Data Security in IoMT

Sathya D(✉), Veena S, Sangamesh Ramesh Yankanchi, Soujanya Manasa

RV University, Bengaluru, Karnataka, India

sathyad@rvu.edu.in

ABSTRACT

The Internet of Medical Things (IoMT), also known as healthcare IoT, consists of interconnected medical devices and applications that enable remote monitoring of patients with chronic conditions. In existing healthcare systems, data from IoMT devices is stored in the cloud for analysis. However, major challenges include ensuring data privacy and prioritising critical health information. Rapid processing and transmission of emergency health data to hospitals are crucial for timely care, while strict privacy measures are necessary to prevent risks like data breaches, fraud, and unauthorised access to medical services. To overcome these challenges, the proposed system implements Ethereum blockchain technology and an edge AI classification algorithm on data collected in real-time. Edge computing enables instant analysis, classification, and prioritisation of health data, minimising latency and facilitating quick decision-making. Simultaneously, blockchain technology ensures robust data privacy through a secure access control mechanism. Patient information is securely stored on the blockchain and accessed via an Aadhaar card number and unique tokens. These tokens enable role-based access control, allowing authorised individuals—like doctors, nurses, patients, and relatives—to view, update, or delete specific records as needed.

KEYWORDS

Edge AI computing, blockchain, Ethereum, Internet of Medical Things (IoMT), cloud storage

1 INTRODUCTION

In the coming years, billions of sensing devices will be connected to the internet as part of the Internet of Things (IoT) ecosystem [1]. This vast network of interconnected devices is expected to generate and access enormous amounts of data, paving the way for innovative applications. However, the scale of this data exchange introduces significant security and privacy challenges, which may impede the further growth and adoption of IoT technology. As device prices continue to decrease and their processing and networking capabilities improve, the number of connected devices is anticipated to steadily rise [2]. The IoT has revolutionised healthcare by introducing wearable devices that enhance medical services [3]. In addition to IoT, the development of

Sathya, D., Veena, S., Sangamesh Ramesh, Y., Soujanya, M. (2025). Edge Computing and Blockchain-Based Data Security in IoMT. *International Journal of Online and Biomedical Engineering (iJOE)*, 21(6), pp. 124–140. https://doi.org/10.3991/ijoe.v21i06.54403

Article submitted 2025-01-13. Revision uploaded 2025-02-11. Final acceptance 2025-02-11.

5G technology has significantly advanced collaborative health tech solutions. Remote sensing in healthcare has been widely validated through various case studies and practical implementations [4]. One of the innovations in the field of IoT in healthcare is continuous monitoring and tracking of patient data, like ECG, blood pressure, and pulse. Such devices can also capture environmental health factors like humidity and temperature through sensors connected to the patient. The collected data is then transmitted to healthcare centres for analysis, including telemedicine applications [5]. As a result, the IoMT encompasses mobile phones, sensors, and wearable devices designed for real-time data collection from patients across diverse settings [6].

In IoMT, data from sensors are typically sent to the cloud for processing. Cloud computing has advanced significantly, enabling cost-effective remote health monitoring. Traditional methods of health surveillance are often impractical and inefficient for real-world implementation [7]. Meanwhile, a method is introduced for remote monitoring with movement detection, incorporating an adaptive sensing approach to reduce costs by leveraging cloud technology [8]. Since timely answers are necessary for efficient care, health monitoring is extremely sensitive to delays, in contrast to other offloading systems. To address this, cloud servers can provide effective assistance, though communication delays remain a concern.

This issue is mitigated by Edge computing, which helps reduce latency. In [9], a healthcare model that integrates edge computing to deliver cost-effective healthcare services is proposed. Their architecture includes server connections, distribution of healthcare analytics, and virtualised deployment. They also introduce an optimisation model solved using a heuristic linear regression method.

To address the emerging concerns, blockchain technology, a forward-looking solution, is being increasingly utilised across various sectors, including healthcare [10]. Blockchain technology is utilised in this industry to safeguard patient records and make it possible for laboratories, pharmaceutical firms, healthcare providers, and other pertinent parties to securely share medical data. By integrating blockchain, the healthcare industry can improve the efficiency, safety, and transparency of medical data exchange. Medical institutions stand to benefit from this technology, as it offers deeper insights and enhances the analysis of patient records [11]. The current health systems struggle with issues of data privacy, processing efficiency, and prioritising urgent medical information.

Our suggested approach addresses these issues by fusing blockchain technology to provide enhanced security with edge computing for efficient data prioritisation. By utilising edge computing, patient data is analysed, classified, and prioritised locally before being sent to the server. This reduces latency and enables quick decision-making, ensuring that critical medical information is processed and acted upon without delay. Data privacy is greatly enhanced by storing the prioritised data on a blockchain, which offers a decentralised, impenetrable system that guards against unwanted access.

To classify patient data according to urgency, we have used a number of machine learning (ML) algorithms, like logistic regression (LR), decision trees, random forests, and SVM classifiers. We assessed these models' performance and found that the SVM classifier produces the best outcomes. This SVM model, which was trained on the Kaggle "Heart Failure Prediction Dataset," is currently being utilised to examine patient data in real time. Doctors and other pertinent medical personnel are promptly notified of urgent instances that the classifier flags for prompt attention and intervention.

In addition to top priority for data security, our solution uses a blockchain-based access control system in order to grant access rights to authorised users like physicians, nurses, patients, family members, and hospital technicians. This improves security and privacy by ensuring that only the right people with the proper authorisation

can view critical patient data. Our solution offers an all-encompassing method for enhancing data privacy, efficiency, and reaction times in healthcare by combining the fast-processing power of edge computing with the safe structure of blockchain.

2 RELATED WORK

In [12], the oversampled quintuple feed forward network (OQFFN), a deep learning technique, was applied to real-time data and the Kaggle public dataset, "Heart Failure Prediction Dataset". A Raspberry Pi edge device performs predictive intelligence before transmitting reports to the server. Various ML and deep learning models were evaluated, all demonstrating strong performance. However, the OQFFN model outperformed and provides an accuracy of 89.25%. This system's key advantage lies in its built-in alerts and the ability to provide precise, real-time heart disease predictions at the edge. However, running more complex deep learning algorithms requires substantial processing power.

In [13], a heart disease prediction model was implemented using bidirectional long short-term memory (Bi-LSTM) and trained on the Cleveland and Hungarian datasets. The original dataset, consisting of 303 instances, was synthetically expanded to 100,000 records, achieving an accuracy of 98.86%. The IoT cloud-based healthcare system demonstrates high predictive performance but lacks edge computing capabilities and secure data access mechanisms.

In [14], a study employed three ML models—LR, random forest, and K-nearest neighbour—for heart disease prediction. To enhance performance, the researchers suggested integrating random forest with a LR grid. The model achieved an accuracy of 82.96% on the Cleveland and Hungarian datasets. However, data privacy remains a concern.

In [15], proposed an energy-efficient smart health system for seizure detection using fuzzy categorisation. The system processes raw EEG data at the edge before transmitting it to the mobile health cloud (MHC), significantly reducing energy consumption by minimising data transfer while maintaining high classification accuracy. Experimental results demonstrated a 60% increase in battery life, and the categorisation rate exceeds 98%.

In [16], edge computing and cognitive computing were integrated to develop a smart healthcare system based on edge cognitive computing. This system optimises resource allocation by prioritising higher-risk patients for edge computing resources. Empirical testing confirmed improvements in both energy efficiency and user quality of experience. However, both systems lack robust mechanisms to protect user privacy [15] [16].

In [17], proposed a secure framework based on blockchain edge computing, which addresses issues of data privacy, integrity, and real-time processing in healthcare IoT. The architecture comes with the incorporation of permissioned blockchain, cryptographic security SHA-256, and data filtering. Performance was tested on a virtualised Ethereum network using various tools, like Solidity and Web3.js. Advantages include enhanced security, very low latency, efficient data handling, and user-centric monitoring. However, one of the challenges with the framework is scalability, high computation, integration complexity, and dependence on participation from users.

In [18], the medical-edge-blockchain (MEdge-Chain) framework is a comprehensive system that combines edge computing and blockchain technologies to efficiently process large volumes of medical data. The framework features an automated patient monitoring system deployed at the edge, enabling remote monitoring and the prompt detection of critical medical events. Additionally, the system integrates this monitoring approach with a blockchain architecture to enhance the efficiency of medical data exchanges among diverse entities. A blockchain-based optimisation model is also

developed to reduce latency and computational costs associated with data transfer, ensuring the delivery of effective and secure healthcare services. The system shows the simulation results and lacks edge implementation on a real hardware system.

An advanced framework combines federated learning, blockchain, actual time-deep learning model, and intrusion detection management to enhance healthcare systems. Federated learning ensures data privacy, blockchain secures decentralized storage, and IoMT devices enable real-time data processing, achieving 97.13% accuracy for intrusion detection and 93.89% for disease diagnosis using the Parkinson's dataset. Benefits include improved security, scalability, real-time monitoring, and reduced data leakage. Challenges involve integration complexity, high computational costs, scalability trade-offs, and limited generalisability due to dataset dependence. The framework outperforms existing models, offering a robust and efficient healthcare solution [19].

A federated learning framework with edge computing enhances privacy and anonymity in IoMT applications. It employs differential privacy with Laplacian noise, hybrid encryption, and partial gradient transfer to reduce data vulnerability. The multi-tier architecture with edge servers lowers server load and protects user identities. Tested with MLP and lightweight CNN on standard datasets, it showed less than 10% accuracy loss from gradient and client reduction. Benefits include improved privacy, reduced data load, and better security, with limitations in accuracy and scalability for larger IoMT networks [20].

In [21], it outlines a multi-layered framework of security that is offered by edge computing to address vulnerabilities in resource-constrained IoMT networks. It integrates lightweight security systems at the IoMT end-device layer, ML-based network intrusion detection systems at the edge, and centralised orchestration in the cloud. The framework is implemented using an LSTM model at the edge, which is of 80% accuracy, and a one-class SVM at the IoMT end-device, which is of 82% accuracy. The distributed strategy compared with the traditional centralised approaches reveals higher adaptability and low overheads in terms of performance. Benefits are there in terms of high scalability and real-time responsiveness that supports constrained devices. And the cons are there are moderate levels of precision. It depends on computationally intensive edge infrastructure.

The SEoT framework is a secure health monitoring system built on edge of things, with high efficiency in terms of a health observing system. Clustering-based abnormality detection for bio signals is implemented on edge and attribute-based encryption implemented on cloud to provide safe access to data. The experimental validation used the multimodal body sensing data of MHEALTH and evaluated clustering algorithms like K-means clustering, all nearest neighbours, first nearest neighbours, and K-Medoid based nearest neighbours. KMNN gained an accuracy of 98.5%. The developed framework addresses challenges like low latency, data confidentiality, and access control in an improved response time, which is robustly covered. However, the system has yet to be implemented with real-time health data and does not differentiate between emergent and general health data [22].

3 METHODOLOGY

The project combines edge computing and blockchain technologies to ensure the security in the IOMT. The AD8232 heart monitor and pulse sensors are used for collecting critical health information from patients. The sensors are interfaced with an Arduino Uno that collects data and is responsible for sending the data to an edge device. There will be an instance of an ML classification model running on this edge device to process this information. Edge computing comes into play here to ensure that

all data processing occurs locally, reducing latency for real-time health monitoring, an important parameter in critical healthcare scenarios where timely analysis can be crucial in saving lives. The information is then recorded on a blockchain, which secures the records and makes them impossible to change. Blockchain technology adds an extra level of security and makes the data verifiable, thus guarding the integrity of sensitive health information. It also offers an access control mechanism that further secures the system, allowing access only to persons with the due authority: health professionals, emergency response teams, and family members who may need information relevant to their roles. This holistic approach to health record management goes a long way toward securing patient privacy and improving the healthcare system's overall dependability and credibility. Figure 1 shows the proposed system flow diagram.

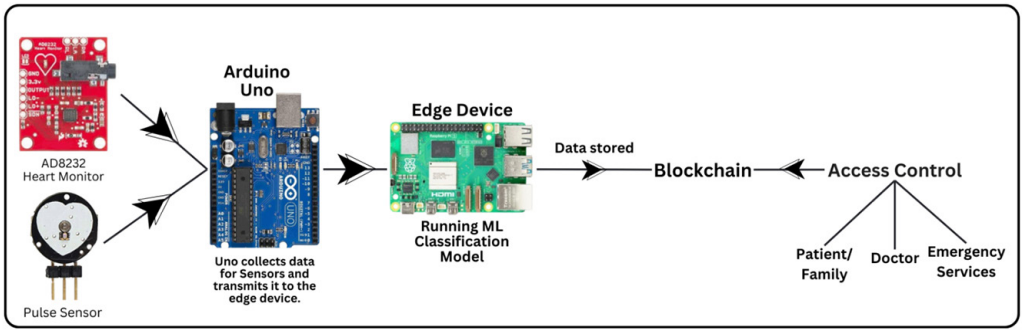

Fig. 1. Proposed system flow

The proposed system is divided into three modules. They are:

1. IoMT – used for collecting real-time data for detecting cardiac abnormality with ECG and pulse sensors
2. On Edge – Classifies emergent data using ML algorithms
3. Blockchain – Enhances data privacy with access control

3.1 Dataset preparation

The heart failure prediction dataset is used for training the proposed edge intelligent system. This dataset is an integration of five different previously separate heart disease datasets. The data now constitutes the largest heart disease dataset ever compiled to date, with 918 unique observations across 11 common features. Datasets used for curation are Cleveland, with 303 observations; Hungarian, with 294 observations; Switzerland, with 123 observations; Long Beach VA, with 200 observations; and Stalog (Heart) data set, with 270 observations. After removing 272 duplicate records, the final dataset is a comprehensive resource for conducting research and analysis on heart disease.

Figure 2 shows the pair plot of key numerical features in the heart failure prediction dataset, revealing several important relationships. Age shows a clear distinction between individuals with heart disease (orange) and those without, with heart disease cases typically being older, supporting age as a significant risk factor. Resting blood pressure does not exhibit a notable trend in relation to heart disease, suggesting limited predictive value. Cholesterol levels show some overlap between the two groups, but slightly higher levels are more common in heart disease cases. Fasting blood sugar, being binary, shows a clearer separation, with higher values (>120 mg/dl) more often seen in individuals with heart disease. The maximum heart rate achieved is more varied in non-heart disease cases, whereas heart disease

patients tend to have lower values. Lastly, higher ST depression (Oldpeak) values are strongly associated with heart disease, highlighting it as a key indicator.

Figure 3 shows the correlation heatmap, which reveals several notable relationships between dataset features, particularly with respect to heart disease. A moderate positive correlation is observed between age and heart disease (r = 0.28), indicating older individuals are more likely to have heart disease. Similarly, fasting blood sugar shows a moderate positive correlation (r = 0.27), suggesting higher fasting blood sugar levels are linked to heart disease. The strongest positive correlation (r = 0.40) is between ST depression (Oldpeak) and heart disease, highlighting it as a significant indicator. Conversely, maximum heart rate achieved exhibits a moderate negative correlation (r = –0.40) with heart disease, indicating that individuals with lower maximum heart rates are more likely to be affected. Resting blood pressure and cholesterol show weak correlations with heart disease (r = 0.11 and r = –0.23, respectively), suggesting limited predictive value. Additionally, age is negatively correlated with maximum heart rate (r = –0.38), meaning heart rates tend to be lower in older people, and cholesterol and Oldpeak are largely independent with a minimal correlation (r = 0.05).

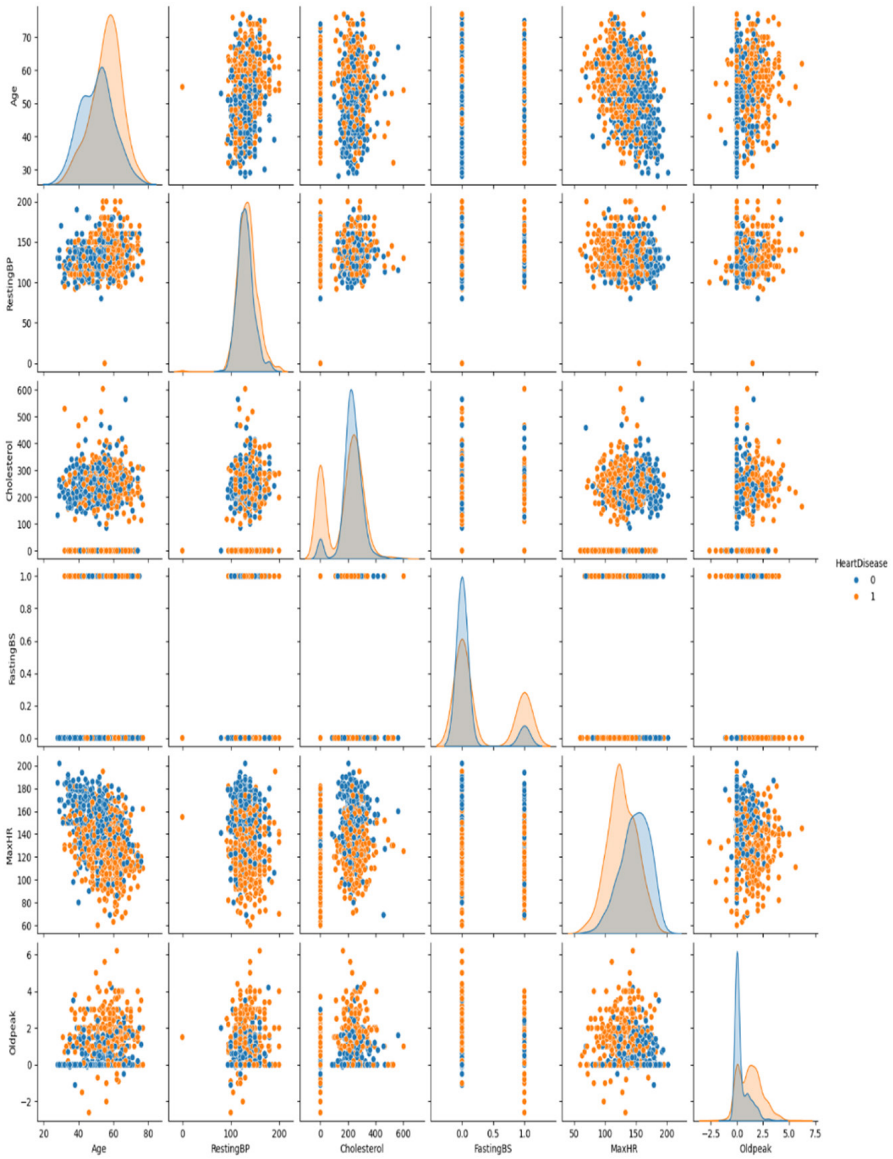

Fig. 2. The pair plot of key numerical features

In order to classify emergent data, we have used these ML algorithms: the LR, decision tree, random forest, and SVM. These algorithms are used first for training the heart disease dataset from Kaggle [23]. Later these algorithms are used for testing the real-time dataset generated by the sensors.

Fig. 3. The correlation heat map

3.2 Machine learning models

This section explores three supervised ML algorithms applied to a heart disease prediction dataset comprising 918 instances with features like age, sex, chest pain type, resting blood pressure, cholesterol levels and more. Each algorithm underwent hyperparameter tuning to optimise its performance for the dataset.

Decision tree classifier. The decision tree classifier is a very straightforward yet powerful supervised learning algorithm that partitions the data into subsets in hopes of minimising the impurity at each split of features. For this dataset, the following hyperparameters were explored and fine-tuned:

- Max_depth: This is the maximum depth of the tree under test. It checks 3, 5, 10 and unlimited depth. In this problem, the value that proved to be optimal is 5. At maximum depth 5, it captured meaningful patterns without overfitting.
- Min_samples_split: Minimal number of samples needed to split a node. Values of 2, 5 and 10 were tested, and the best trade-off between complexity and performance has been offered by 5.
- Min_samples_leaf: Minimal number of samples in each leaf node. 2 was the best value for this problem and is also rather reasonable because the splits are not too focused on particular examples.

Decision trees are very intuitive, but they tend to overfit if allowed to grow too deep. Limiting depth and tweaking the splitting criteria can make it easier to avoid this overfitting.

Random forest classifier. The random forest classifier is an ensemble technique, summarising the predictions of multiple decision trees combined to make it more accurate and general. It was introduced in 1995 by Tin Kam Ho, and random forest particularly deals well with well-structured data and is less likely to overfit compared to standalone decision trees.

Hyperparameters fine-tuned in this model are:

- n_estimators: The number of decision trees in the forest. Values of 50, 100, and 200 were tried, and 200 was chosen with a balance between accuracy and no overfitting.
- max_depth: capped at 5 to avoid too much complexity but keep the scope of predictiveness
- min_samples_split: Best to achieve optimal splits across nodes for 5.
- min_samples_leaf: Set to 2 to not generate overly specialised trees.
- max_features: This parameter specifies the number of features to be used in splitting a node. The "sqrt" option was optimal for this dataset since it resulted in efficient and stable splits.

Using the ensemble-based decision, the random forest performed well, in fact better than the individual decision tree.

Support vector machine. Algorithm: SVM is the earliest algorithm proposed by Vladimir Vapnik in 1992 for the classification of classes in high-dimensional spaces using hyperplanes. Its usage is mostly seen in the case presented above with smaller-sized datasets and features with scale differences.

Given below is the SVM model used as the predictive model for heart disease:

- C: This is the regularisation parameter. It controls the trade-off between large margin and minimum misclassification error. The default value of 1.0 yielded the best results.
- Kernel: This kernel selects a function to map the data into higher dimensions. The radial basis function (RBF) kernel was chosen for its effectiveness in dealing with non-linear relationships.
- Gamma: The strength of individual data points. Set automatically, depending on the feature distribution of the dataset.

Since SVM relies on the support vectors rather than using the whole data in its computation, it is computationally efficient and less prone to overfitting for binary classification tasks like this.

Logistic regression. The LR classifier is a widely used supervised ML algorithm in the framework of binary classification problems, for example, heart disease prediction. It uses a logistic function in the modelling of the relationship between one or more independent variables (features) and the dependent variable (target), outputting probabilities for classification. Its strength lies in its simplicity in instances in which the relationship between variables is linear. Hyperparameter tuning included the following different values in an attempt to optimize the model.

C (Regularisation strength): It is the strength of the regularisation strength that acts against overfitting through penalising coefficients. It is stronger with smaller

values. From experimentation, the value of C was set at 1 since it gave a good balance between bias and variance for the dataset.

Solver: Optimisation solver used to fit the LR model. Some of them that have been tested are:

- newton-cg: good for multi-class as well as large datasets.
- lbfgs: useful when datasets are very small in size, default parameters used.
- liblinear: good for small datasets or where features present in the dataset are sparse.

For the suggested prediction model, the solver 'lbfgs' was selected using cross-validation results.

Random_state: This parameter ensures that the output is reproducible by controlling the randomness in the algorithm. For the experiment, the random_state was set to 42 for outputting a consistent result during different runs.

Max_iter: The maximum number of iterations that would be allowed for the optimisation algorithm to converge. max_iter was set to 1000, and this ensured that the solver converged even on complex datasets.

The LR model used GridSearchCV for hyperparameter optimisation. It tried all possible combinations of hyperparameters. Then, it was tuned with improved accuracy and other performance metrics so that the model could be an appropriate solution for the task of heart disease prediction.

3.3 Blockchain

Blockchain acts as an access control mechanism securely to manage patient data records.

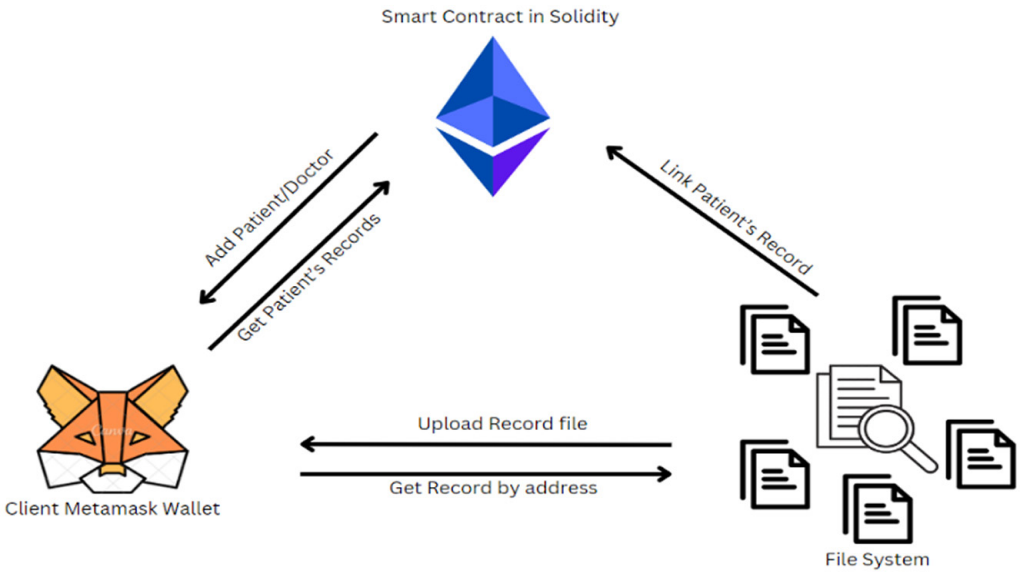

Fig. 4. Working of smart contract

Blockchain is a kind of decentralised and distributed ledger which provides full security, transparency and immutability. These characteristics make it one of the

perfect solutions to tackle sensitive health care data where privacy, security and control over data access are crucial.

- Security: Blockchain applies such a level of cryptography that no data is allowed to be altered or tampered with. This maintains the integrity of the patient's health records.
- Transparency: Blockchain maintains the record of every transaction-being the history of access to patient data-and also ensures that only authorised people can access parts of the data.
- Decentralisation: The presence of no central body that controls the data allows patients to be more in control and avoids the risks of systems based on central cloud storage, like being hacked or data breaches.

Blockchain for access control. While blockchain in this system doesn't act just as a medical record ledger but as an access control system, it can leverage blockchain's smart contracts to create user-specific roles, including doctors, nurses, or family members. Figure 4 represents the working of the smart contract.

- Doctors might have full access to the complete patient's medical history for update, addition, or deletion.
- The nurse might have access which allows editing some data, like vital signs, but does not grant them allowance to view sensitive history.
- Relatives may hold a read permission, which entails permission to view basic health information but does not allow modification.

Blockchain-based authorisation. These tokens are generated based on Aadhar number for unique identification in India and smart contracts. Each smart contract defines who has access to what data under what conditions. In case someone tries to fetch any information of the patient, blockchain checks for the following:

- Who is trying to see the patient's information: doctor, nurse, or family member?
- What level of access does he/she get?

The request of access by doctors anytime for emergency data and family members under specific conditions that need to be determined in the smart contract.

Data privacy and control. Blockchain thus provides a very secure storage of a patient's data, while access is granted only to those authorised through the use of unique tokens. The following can, therefore, be assured in this system:

- Data exposure limited: Only the information needed would be given to the person concerned and at the right time. For instance, all of the medical data is not provided to a family member. This will ensure patients' privacy in that regard.
- Traceability: All the data accesses are recorded on a blockchain. The logging must, in particular, be traceable about who accessed or altered the data.
- Decentralized data management: Since the data is kept in a distributed nature on the blockchain, there isn't one single point of failure that gives way to data leakage.

Access control with blockchain in place provides secure and traceable role-based access to sensitive medical data. This adds an extra layer of tokens and smart contracts, hence providing a flexible and reliable approach for the various needs for access by doctors, nurses, family members, and others while guaranteeing data privacy and integrity.

4 RESULTS AND DISCUSSION

4.1 IoMT- ECG and pulse sensor connection

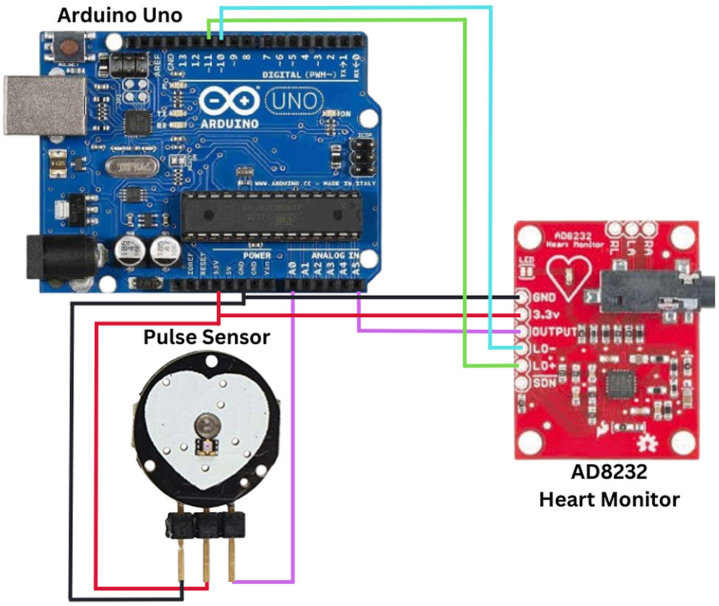

Fig. 5. Schematic diagram of Arduino connection with heat rate and pulse sensor

Figure 5 illustrates the schematic connections of the Arduino Uno, pulse sensor, and AD8232 heart monitor wiring. The Arduino Uno acts as the base microcontroller. It receives input signals from the AD8232 heart monitors and the pulse sensor. Three cables link the pulse sensor to the Arduino: the purple wire goes to the A0 analogue input pin for the pulse signal itself, the black wire goes to the GND pin those grounds it, and the red wire goes to the 5V pin to power it. The AD8232 heart monitor similarly gets connected with its 3.3V power pin to the Arduino's 3.3V output, GND to ground on the Arduino, and its OUTPUT pin to the Arduino's analogue input pin for acquiring the signal. Moreover, the SDN (shutdown) pin has not been connected to anything; thus, the module remains in the active state. The setup is such that it will enable the Arduino to monitor heart rate data from both the pulse sensor and the AD8232 heart monitor.

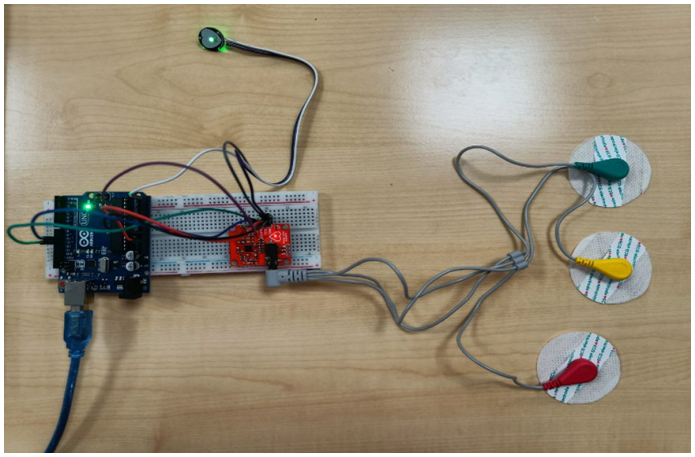

Fig. 6. Pulse and ECG sensor connection

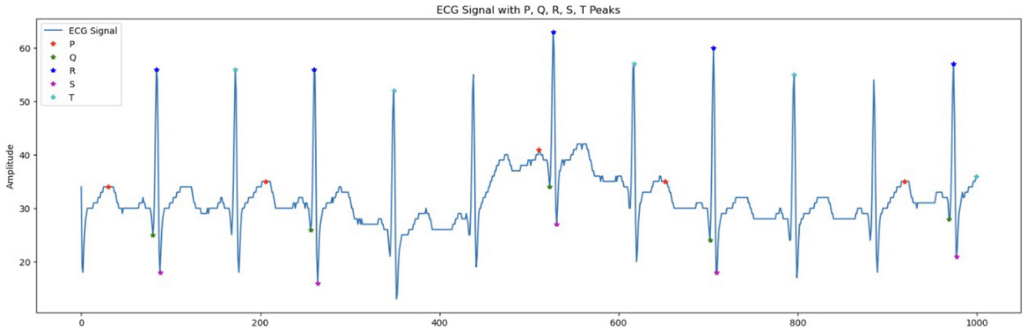

Fig. 7. ECG pulse

As shown in Figure 6, the pulse sensor and the ECG monitor sensor are connected to an Arduino Uno from where the data can be collected. Below Figure 7 is a graph of ECG and pulse obtained by running the Arduino code.

4.2 Edge deployment on ESP32

The deployment of an ML model, trained on the heart disease dataset, onto an ESP32 microcontroller and tested using a collected real-time dataset. We used the Heart Disease Dataset, which contains demographic, clinical, and laboratory features to predict the probability of heart disease. The dataset was pre-processed by encoding categorical variables, normalising numerical features, and balancing class distributions. The data was split into training, validation, and testing subsets to ensure a comprehensive and reliable evaluation. Some of the key features of the TensorFlow-built ML model, hereby implemented using the MLP architecture in a task of binary classification:

- Input layer: 11 features that are already pre-processed enter.
- The "hidden layers" section consists of three dense layers with ReLU activation, batch normalisation, and dropout for regularisation.
- The output layer consists of one neurone with a sigmoid activation function that calculates the probability.

The Adam optimiser and binary cross-entropy loss function were employed in the training model. The data was balanced by the use of class weighting. Following training, the model's test accuracy was 89.87%.

TFLite conversion: This model was converted to TFLite format for the ESP32 deployment. Conversion does further optimisation of the model by compacting it and preparing the same for microcontroller environments, thereby further processing it into a C header to be used with ESP32 firmware.

Edge deployment on ESP32: We deployed the inference pipeline on an ESP32 using the Eloquent TinyML library. The firmware comprises

- Model integration: Integrating the TF Lite model as a C array.
- Input handling: Pre-processed feature inputs are fed into the model.
- Inference execution: The ESP32 executes local predictions, outputting heart disease likelihood.
- Results visualisation: Classes and confidence scores of the predicted classes are shown through a serial monitor.

Five samples are tested across the range of the dataset to test its deployment. All samples were classified correctly, with the outputs by the ESP32 matching those of the TensorFlow.

4.3 Results and key findings

- The ESP32 achieved real-time inference with minimal latency, demonstrating its suitability for edge applications.
- The deployed model's predictions aligned with those made during the Tensor Flow testing phase, ensuring reliability.
- The optimized memory usage (TENSOR_ARENA_SIZE: 5KB) highlights the ESP32's ability to run resource-constrained ML models.
- This experiment underscores the potential of edge computing for secure and efficient healthcare monitoring. Figure 8 shows Edge deployment on ESP32.

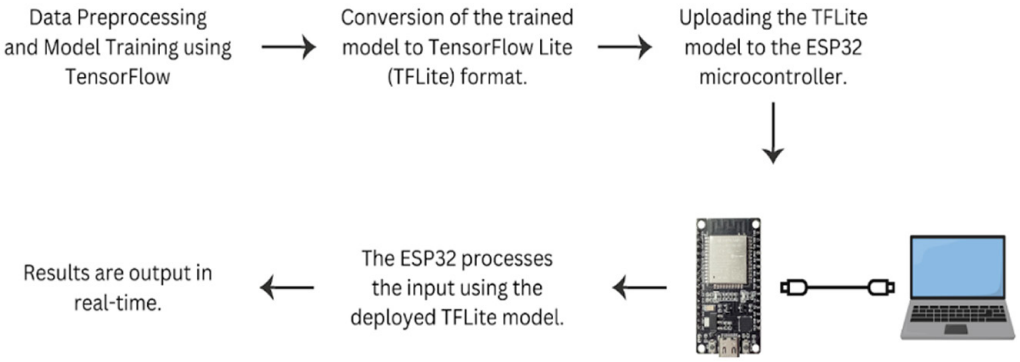

Fig. 8. Edge deployment on ESP32

4.4 Model performance evaluation

The decision tree classifier, random forest classifier, support vector machine, and LR models were evaluated in a hold-out test set and accuracy, precision, recall, and F1-score metrics. The evaluation appears to indicate that both random forest and SVM served well to provide great performance, although SVM was marginally better at F1-score compared to RF.

- Decision tree classifier: This method too delivered a strong performance. However, it was not as accurate and not as generalizable as compared to ensemble-based and kernel-based methods.
- Random forest classifier: Balanced high accuracy, precision and recall, most reliable.
- SVM: Best overall performance with high scores on all metrics, benefits from its robust handling of non-linear decision boundaries.
- Logistic regression: Strong and stable did awesome in all those scenarios in which the relationship between features and the target variable was roughly linear. Its simplicity and interpretability made sure effective regularisation insured robustness with competitive scores in all the metrics. Table 1 represents the performance comparison on real-time dataset using ML models.

Table 1. Performance comparison on real time dataset

Prediction Model	Test Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Decision Tree Classifier	85.8	93.1	82.3	87.3
Random Forest Classifier	88.4	91.2	89.0	90.1
Support Vector Machine	88.7	91.3	89.6	90.4
Logistic Regression	87.6	92.2	86.5	89.3

4.5 Privacy preservation using blockchain

The access control interface for a health monitoring system designed for blockchain-based data security in the IoMT. The interface allows for secure login by either a doctor or a family member, who can then access the patient's medical data stored on a blockchain. This ensures that only authorised users can view sensitive medical information, thus enhancing data privacy and security through robust access control mechanisms. Our Solana-Powered Blockchain Medical Storage System is a cutting-edge solution for securely storing and managing medical records. It uses Solana's blockchain's speed and efficiency for lightning-fast data transfers and Pinata and IPFS for decentralised, tamper-proof data storage. Using zero-knowledge proof, users can securely enter their medical data, assuring data privacy and protection.

Compliance with healthcare data privacy requirements, like HIPAA and GDPR, is essential to our system, preserving the confidentiality of patient information. Our solution is cost-effective and can accommodate the growing amount of medical information and users due to its scalable architecture and reduced transaction costs. It is the healthcare data management system of the future, combining speed, security, and limited access to fulfil the demands of both healthcare professionals and patients.

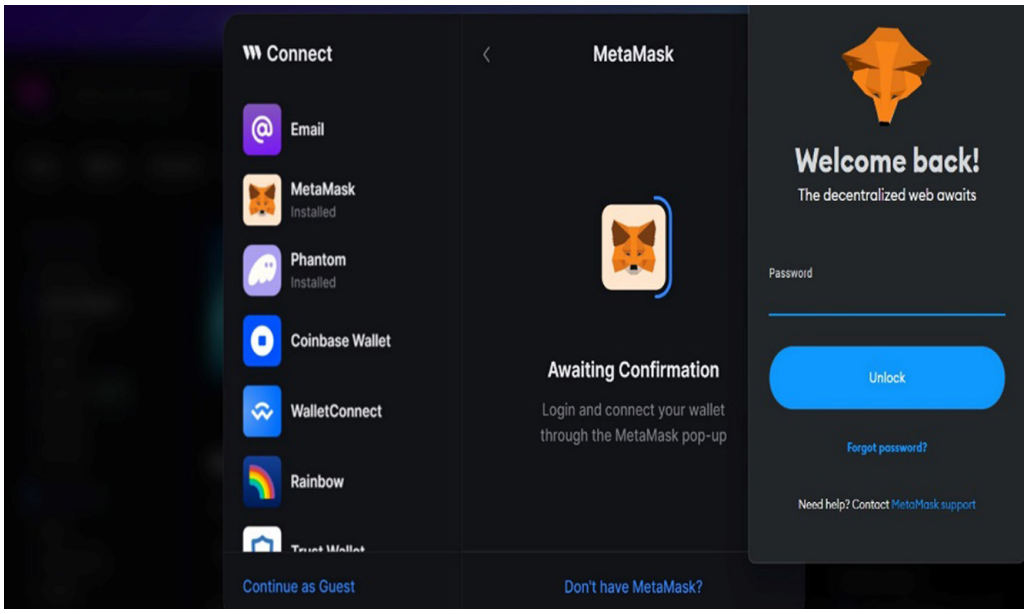

Fig. 9. Login screen

Our system provides several login choices for authentication and access control. Users can log in with cryptocurrency wallets for extra protection, Google or email

credentials for convenience, or even Aadhar card verification for a strong access point. This multifaceted method to log in ensures that sensitive medical records are only accessed by authorised personnel, as shown in Figure 9.

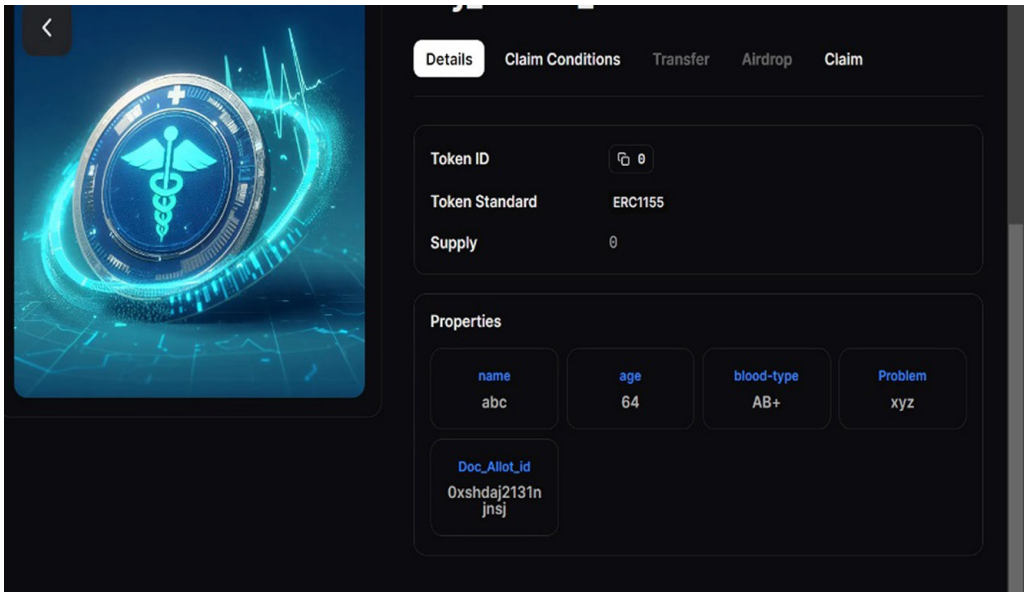

Fig. 10. Token-based access control

Our Solana-Powered Blockchain Medical Storage System includes token-based access control, an innovative security feature that offers an extra degree of protection to medical record management. To obtain access to specific data or functionality within the system, users must give a unique token or cryptographic key with token-based access control. This token, often generated during the authentication process, serves as a digital passkey that validates the user's identity and permissions. It ensures that only authorised individuals can view or modify certain medical records or perform specific actions, adding an extra level of security to the system. Token-based access control is a key component in safeguarding sensitive healthcare data and preventing unauthorised access, as shown in Figure 10.

By implementing token-based access control, our system strengthens its data privacy measures and bolsters the overall security of medical records, meeting the highest standards of compliance and confidentiality in the healthcare industry.

5 CONCLUSION

The system uses Edge AI to quickly analyse and prioritise important health data, making sure it reaches medical professionals in time for emergency care. This reduces delays by relying less on cloud processing and helps in making quick decisions that can save lives. It also uses the Ethereum blockchain to keep patient data secure, allowing access only through Aadhaar-linked tokens. This ensures that sensitive health information is safe from unauthorised access. Overall, the proposed system improves healthcare by making it faster, safer, and more reliable for patients. The proposed system can be further enhanced to integrate with IoT systems deployed for patient monitoring in hospitals. Additionally, edge computing combined with blockchain-based security is well-suited for other IoT applications requiring enhanced security and rapid data processing.

6 REFERENCES

[1] H. Liao *et al.*, "Learning-based context aware resource allocation for edge-computing-empowered industrial IoT," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4260–4277, 2020. https://doi.org/10.1109/JIOT.2019.2963371

[2] M. Ma, A. Liu, and X. Chen, "Dynamic power management and adaptive packet size selection for IoT in e-Healthcare," *Comput. Electr. Eng.*, vol. 65, pp. 357–375, 2018. https://doi.org/10.1016/j.compeleceng.2017.06.010

[3] C. Bhatt and Y. Bhatt, "Internet of things in healthcare," in *Internet of Things and Big Data Technologies for Next Generation Healthcare. Studies in Big Data*, vol. 23, C. Bhatt, N. Dey, and A. Ashour, Eds., Springer, Cham, 2017, pp. 13–33. https://doi.org/10.1007/978-3-319-49736-5_2

[4] M. Amani *et al.*, "Google earth engine cloud computing platform for remote sensing big data applications: A comprehensive review," *IEEE J. Sel. Top. Appl. Earth Observations Remote Sens.*, vol. 13, pp. 5326–5350, 2020. https://doi.org/10.1109/JSTARS.2020.3021052

[5] E. Absalom and O. Taiwo, "Smart healthcare support for remote patient monitoring during covid-19 quarantine," *Inf. Med. Unlocked*, vol. 20, p. 100428, 2020. https://doi.org/10.1016/j.imu.2020.100428

[6] M. Shagiq, "Advances in IoMT for healthcare system," *Sensors*, vol. 24, no. 1, p. 10, 2024. https://doi.org/10.3390/s24010010

[7] W. Shi, J. Cao, Y. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 637–646, 2016. https://doi.org/10.1109/JIOT.2016.2579198

[8] J. Pagán *et al.*, "Toward ultra-low-power remote health monitoring: An optimal and adaptive compressed sensing framework for activity recognition," *IEEE Trans. Mob. Comput.*, vol. 18, no. 3, pp. 658–673, 2017. https://doi.org/10.1109/TMC.2018.2843373

[9] L. Gu, D. Zeng, S. Guo, A. Barnawi, and Y. Xiang, "Cost efficient resource management in fog computing supported medical cyber-physical system," *IEEE Trans Emerg Top Comput.*, vol. 5, no. 1, pp. 108–119, 2017. https://doi.org/10.1109/TETC.2015.2508382

[10] H. S. A. Choi, "Longitudinal healthcare data management platform of healthcare IoT devices for personalized services," *J. Universal Comput. Sci.*, vol. 24, no. 9, pp. 1153–1169, 2018.

[11] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, and K. Mankodiya, "Towards fog-driven IoTeHealth: Promises and challenges of IoT in medicine and healthcare," *Future Gener. Comput. Syst.*, vol. 78, pp. 659–676, 2018. https://doi.org/10.1016/j.future.2017.04.036

[12] Md. Ishan Arefin Hossain, A. Tabassum, and Z. U. Shamszaman, "Deep edge intelligence-based solution for heart failure prediction in ambient assisted living," *Discover Internet of Things*, vol. 3, no. 11, 2023. https://doi.org/10.1007/s43926-023-00043-4

[13] A. A. Nancy, D. Ravindran, P. M. D. Raj Vincent, K. Srinivasan, and D. Gutierrez Reina, "Iot-cloud-based smart healthcare monitoring system for heart disease prediction via deep learning," *Electronics*, vol. 11, no. 15, p. 2292, 2022. https://doi.org/10.3390/electronics11152292

[14] M. Kumar *et al.*, "Autonomic edge cloud assisted framework for heart disease prediction using rf-lrg algorithm," *Multimedia Tools and Applications*, vol. 83, pp. 5929–5953, 2024. https://doi.org/10.1007/s11042-023-15736-9

[15] A. Awad Abdellatif, A. Emam, C.-F. Chiasserini, A. Mohamed, A. Jaoua, and R. Ward, "Edge-based compression and classification for smart healthcare systems: Concept, implementation and evaluation," *Expert Systems with Applications*, vol. 117, pp. 1–14, 2019. https://doi.org/10.1016/j.eswa.2018.09.019

[16] M. Chen, W. Li, Y. Hao, Y. Qian, and I. Humar, "Edge cognitive computing based smart healthcare system," *Future Generation Computer Systems*, vol. 86, pp. 403–411, 2018. https://doi.org/10.1016/j.future.2018.03.054

[17] Rabeya Bosri *et al.*, "HIDEchain: A user-centric secure edge computing architecture for healthcare IoT devices," in *IEEE INFOCOM 2020 – IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2020. https://doi.org/10.1109/INFOCOMWKSHPS50562.2020.9162729

[18] A. A. Abdellatif *et al.*, "MEdge-chain: A holistic framework for medical data exchange using edge computing and blockchain," *IEEE Internet of Things Journal*, vol. 8, no. 21, pp. 15762–15775, 2021. https://doi.org/10.1109/JIOT.2021.3052910

[19] J. Almalki, S. M. Alshahrani, and N. A. Khan "A comprehensive secure system enabling healthcare 5.0 using federated learning, intrusion detection and blockchain," *PeerJ Computer Science*, vol. 10, p. e1778, 2024. https://doi.org/10.7717/peerj-cs.1778

[20] Akarsh K. Nair, J. Sahoo, and E. D. Raj, "Privacy preserving Federated Learning framework for IoMT based big data analysis using edge computing," *Computer Standards & Interfaces*, vol. 86, p. 103720, 2023. https://doi.org/10.1016/j.csi.2023.103720

[21] J. A. A. M. K. Eric Gyamfi, "Network security system in mobile edge computing-to-IoMT networks using distributed approach," *Security and Risk Analysis for Intelligent Edge Computing*, vol. 103, 2023.

[22] A. Singh and K. Chatterjee, "Edge computing based secure health monitoring framework for electronic healthcare system," *Cluster Comput*, vol. 26, p. 1205–1220, 2023. https://doi.org/10.1007/s10586-022-03717-w

[23] Fesoriano, "Heart failure prediction dataset," Kaggle, 2021. https://www.kaggle.com/datasets/fedesoriano/heart-failure-prediction

7 AUTHORS

Sathya D working as Associate Professor in School of Computer Science and Engineering at RV University, Bengaluru, Karnataka, India (E-mail: sathyad@rvu.edu.in).

Veena S working as Assistant Professor in School of Computer Science and Engineering at RV University, Bengaluru, Karnataka, India.

Sangamesh Ramesh Yankanchi studying III-year B.Tech. (CSE) in School of Computer Science and Engineering at RV University, Bengaluru, Karnataka, India.

Soujanya Manasa studying III-year B.Tech. (CSE) in School of Computer Science and Engineering at RV University, Bengaluru, Karnataka, India.