iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.79693

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

IoHT-SHIELD: Blockchain-Assisted Anomaly Detection Framework for Securing IoHT Devices

Muneebullah Hussaini Syed[1], Mohammad Saif[2], Mr. B. J. Job Karuna Sagar[3]
[1, 2]*Department of Artificial Intelligence and Data Science, Methodist College of Engineering and Technology (Affiliated to Osmania University) Hyderabad, Telangana, India*
[3]*Associate Professor, Department of Computer Science and Engineering, Methodist College of Engineering andTechnology, (Affiliated to Osmania University)* Hyderabad, Telangana, India.

Abstract: ***With the rapid proliferation of Internet of Healthcare Things (IoHT), cybersecurity challenges have emerged in the form of resource-constrained and interconnected devices. To overcome these challenges, this project proposes a blockchain-based anomaly detection system that ensures intelligent threat detection, tamper-proof logging, and secure data management. The system utilizes machine learning algorithms such as Isolation Forest, SVM, CatBoost, and LSTM Autoencoders to identify anomalies in data streams generated by Internet of Healthcare Things devices. The system securely logs the anomalies in the Ethereum blockchain and stores data in IPFS to ensure data integrity and decentralization. The system utilizes FastAPI to establish communication with the system and process data in real-time. The results of the proposed system show excellent accuracy and improved security performance against benchmark datasets. The proposed system ensures data security in Internet of Healthcare Things environments in a reliable and transparent manner. Index Terms—Internet of Healthcare Things (IoHT), anomaly detection, blockchain, Ethereum, IPFS, CatBoost, Isolation Forest, LSTM Autoencoder, cybersecurity, data integrity.***
Keywords: Internet of Healthcare Things(IoHT), Blockchain, IPFS, Machine Learning, Deep Learning, Ethereum, and Isolation Forest, LSTM Autoencoder, CatBoost.

I. INTRODUCTION

Internet of Things in the healthcare sector has had a great impact in the healthcare field. Clinicians are now able to monitor their patients remotely via information to make informed decisions. The amount of information from the fitness machines, medical devices, and health care system is enormous. Information makes things quick and efficient. With the application of IoT, one can see that there will be many problems of cyber security. It is quite possible that the information in the health sector will be accessible without authorization and will be subjected to cyber attacks.

Thus, what should be developed is the ability to detect potential threats quickly and secure the information stored in the medical records. The most effective way to achieve this is by discovering some specific patterns. In such a way, any potential threat can be identified instantly. Machine learning solutions are quite good at detecting specific patterns from the datasets. Besides, there is great potential for learning new threats and detecting them in the future. Data integrity plays an important role in the field of healthcare. This indicates that there should be a solution for ensuring data integrity. Blockchain can be used for this purpose. Thus, combining machine learning with blockchain solutions for threat detection and data integrity will be extremely effective. The objective of this paper is to increase reliability, scalability, and trustworthiness of IoHT systems.

II. LITERATURE SURVEY

The process of developing IoHT technologies takes place at a very high rate. The implementation of IoHT technology brings about the application of medical devices that provide real-time monitoring and controlling of health care. On the other hand, cybersecurity has been one of the threats associated with the adoption of IoHT technologies. This is brought about by the interconnectedness of IoHT technologies and the limited availability of resources for them. Traditional approaches have been found ineffective due to their incapability to cope with information. Anomaly detection approaches deal with the detection of anomalies within the system. Some of the scientists who researched the topic of anomaly detection using machine learning are Islam et al. (2023). The scientists designed an algorithm for anomaly detection using machine learning based on CNN and ESA methods. Thus, the algorithm proved to be highly efficient in terms of producing accurate results. There are also some other relevant papers devoted to the same topic, and the paper by Saeed et al. (2023) is among them.

The paper presents a machine learning algorithm that includes SVM and RF classifiers. Talking about the infrastructure as it relates to health care, Mantas et al. (2022) have proposed the IDS model based on anomalies. IDS operates within the framework of the IoMT network. Speaking of the research objectives, it is important to say that providing secured communication of medical devices is the main objective of the study. Nevertheless, while developing their research, the scholars pay particular attention to the importance of security as an integral part of the health care infrastructure.

The following studies on the application of AI and blockchain have been recently conducted. The application of blockchain technology serves as a mechanism where the information could be shared and stored. Blockchain technology would ensure that the information is secure while being kept transparent always. The integration of blockchain technology with AI would provide enhanced security methods. The integrated blockchain system does not have any single point of failure while any activity within the system is recorded. In case of integration of blockchain technology with AI, such methods as SVM, Catboost, and deep learning are utilized. In addition, novel techniques like DNN and Blockchain technologies have emerged, and their efficiency is already proven. Thus, the newly introduced techniques can be regarded as superior when it comes to cyber anomaly detection. Furthermore, the new techniques prevent the occurrence of any type of false predictions. Additionally, the new techniques incorporate the idea of smart contracts during cyber attacks.

Nevertheless, even though there are many advances in this field, there are some drawbacks in the current techniques. Such drawbacks involve expensive computational costs, non-real-time performance, and lack of scalability for large IoHT networks. Most of the existing techniques are centered on anomaly detection or data protection.. There must also be a system that can detect anomalies using machine learning algorithms. In addition, there must be a security architecture that is decentralized in terms of how it handles its information. The security architecture proposed below can be implemented using machine learning methods and blockchain technology.

III. PROPOSED SYSTEM

The proposed system is a Blockchain-Assisted Anomaly Detection Framework for Securing IoHT Devices. This system is designed to address the limitations of traditional IoHT security mechanisms. It combines machine learning-based anomaly detection with blockchain technology to provide real-time threat detection, secure data storage and decentralized trust management for IoHT Devices.

The system has a -layered approach that ensures efficient data processing, accurate anomaly detection and tamper-proof logging for IoHT Devices. This is different from systems that rely on centralized security mechanisms. The proposed framework eliminates points of failure by using decentralized blockchain infrastructure for IoHT DevicesBlockchain Technology has many features that could make IoHT devices more secure. These features include being unchangeable, being open to everyone, and having a distributed consensus. The first step is for the IoHT devices to gather the data they need. The data gathered during this process consists of sensor data, telemetry data, and traffic data from the IoHT devices. The second step is to process the data that was collected. Machine learning forms the backbone of the framework and uses various algorithms such as Isolation Forest, Support Vector Machine, CatBoost, and LSTM Autoencoders for analysis of the data obtained from the IoHT devices. Various algorithms like Isolation Forest, Support Vector Machine, CatBoost, and LSTM Autoencoders are applied on the data obtained from the IoHT devices for detecting any anomalies which deviate from the normal behavior of the IoHT devices. Machine learning has been effective in detecting any cyber attacks because of its capabilities in analyzing huge chunks of data and learning anything instantly. Any anomalies detected using the machine learning algorithms in the IoHT devices will be detected immediately by the blockchain module. As far as other issues are concerned, they are expected to stay the same as before regarding the blockchain module. The main reason for the above lies in the capability of blockchain technology to provide tamper-proof data storage. In other words, whatever has been done with the help of this technology is already documented through the data stored within it. Hence, the use of blockchain technology will become much easier because of the tamper-proof feature. Moreover, any sort of data may be used for storing purposes by the means of IPFS technology. As far as other technologies such as FastAPI are concerned, connections will become much easier. They refer to the connections between the user interface, machine learning algorithm, and blockchain technology. Another important aspect includes the fact that the user interface in the dashboard enables the monitoring of the IoHT device.

IV. SYSTEM ARCHITECTURE

Architecture for Securely Securing the IoHT Devices through Various Processes in the Blockchain-Assisted Anomaly Detection Framework is a technique used to employ several layers to ensure the security of the IoHT devices through different approaches. In this case, the architectural approach is named Blockchain-Assisted Anomaly Detection Framework for IoHT Device Security.

This is because, in the architecture, the collection of data through machine learning algorithms occurs in order to detect any anomaly prior to storing the data in the blockchain.
There is integration of Blockchain technology and artificial intelligence in most IoT devices' security frameworks in which machine learning algorithms analyze data collected from such devices to detect any anomaly.

A. Data Acquisition Layer

The Data Acquisition Layer gets information from IoHT devices. This includes things like sensors and medical devices. The Data Acquisition Layer also gets information from the network.
The Data Acquisition Layer is very important in an IoHT system.The IoHT devices make a lot of information. So the Data Acquisition Layer makes sure it gets the information from the IoHT devices in a way that works and at the time.This is very important because the Data Acquisition Layer helps make sure the information is used in a way that works and on time.The Data Acquisition Layer is a part of this because it gets information from the IoHT devices and other things like device telemetry and network traffic.The Data Acquisition Layer is important for getting information, from the IoHT devices.

B. Data Preprocessing Layer

Now we get the data. Bring it to the Data Preprocessing Layer. The main thing we want to do is get some useful information from the data that can help us with machine learning. We do some work on the data to get it ready, for machine learning. The Data Preprocessing Layer is where we make the data good to use for machine learning. We change the data so it can be used to train the machine learning models. The data we have is changed in the Data Preprocessing Layer so it is ready to use for machine learning.

C. Machine Learning Layer

The Machine Learning Layer is a part of our system. It uses machine learning algorithms like Isolation Forest, Support Vector Machine, CatBoost and LSTM Autoencoders to find anomalies in IoHT data. These models take a look at the IoHT data. They find things that do not seem right. We use the Machine Learning Layer to detect anomalies because it does a job. The Machine Learning Layer learns what is normal. It changes to deal with cyber threats in real time for IoHT Devices. The Machine Learning Layer helps to keep IoHT Devices safe from harm.The Machine Learning Layer is very important.It uses IoHT data to learn and get better. The Machine Learning Layer is the key, to keeping our system secure.

D. Decision and Alert Layer

Based on the anomaly scores from the machine learning models the system decides whether the IoHT data is normal or anomalous. If an anomaly is found it triggers an alert and takes action. This layer makes sure that the system responds to threats in time which improves the security and reliability of the IoHT Devices.

E. Blockchain Layer

The blockchain layer makes sure that anomaly events are stored in a way that cannot be tampered with for the IoHT Devices. Each anomaly that is found is recorded as a transaction in the blockchain, which makes it immutable and transparent. The blockchain gets rid of points of failure and keeps a decentralized record of system activities, which enhances trust and data integrity for the IoHT Devices.

F. Data Storage Layer

To handle amounts of IoHT data the system uses decentralized storage. This method stores data using content-based addressing, which ensures that the data is intact, available and resistant to tampering. It also reduces the need for servers for the IoHT Devices.

G. Application and Visualization Layer

The Application and Visualization Layer is the part of the IoHT cybersecurity solution that we are discussing.It has a web-based dashboard that allows users to see what is currently happening in the system.The Application and Visualization Layer has this web-based dashboard that displays information such as when something's not normal the status of devices how well the system is performing and records of blockchain transactions.When something is not normal in the system the Application and Visualization Layer will notify users through the machine learning models that're part of the Application and Visualization Layer.

We use blockchain to ensure that the data we store is safe and has not been altered.The blockchain part of the Application and Visualization Layer ensures that all the information is transparent and cannot be changed.The Application and Visualization Layer uses intelligence to find anomalies, which helps us examine the threats in the network.The Application and Visualization Layer is very useful for users, system managers and healthcare professionals because it helps them make decisions based on the data the history of transactions and the alerts they receive. The way the dashboard, the application programming interfaces the machine learning model and the technologies that store and share data, such as IPFS and blockchain all work together is very smooth.This makes it easy for users to monitor the IoHT devices. The Application and Visualization Layer makes it easy for users to keep track of their IoHT devices. It is, like a window through which users can see what is happening in the Application and Visualization Layer of the IoHT system.

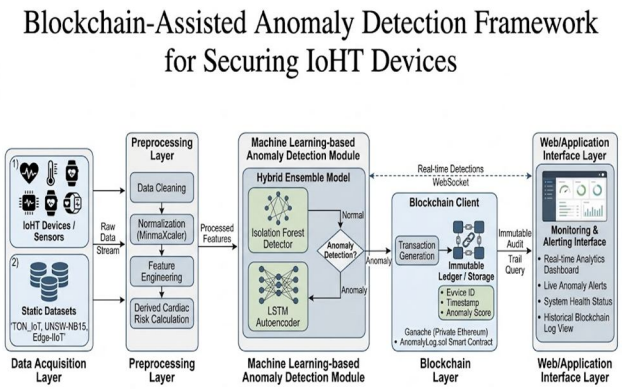


Figure 1: System Architecture of the Proposed Framework

Fig. 1 System Architecture

V. IMPLEMENTATION

Blockchain-Assisted Anomaly Detection Framework for IoHT Device Security implementation depends on the approach we take. This approach uses different parts that work together. They help find patterns in data by studying it with machine learning techniques and blockchain.

The way we implement Blockchain-Based Anomaly Detection Framework for IoHT Devices varies. This method involves using components. When we put them all together they help detect anomalies in data.They also keep IoHT data safe in the blockchain.First we collect data from TON_IoT, UNSW-NB15 and Edge-IIoT IoHT data sets.These data sets have information about IoHT devices and networks. Then we study the data to find any patterns.

We use machine learning and tools like Pandas and NumPy libraries in Python to analyze the data.The Blockchain-Assisted Anomaly Detection Framework helps keep IoHT devices secure. The approach is key, to making it work.We use blockchain to keep data safe.The machine learning techniques help detect anomalies.

The combination of both makes it effective. After the data is ready the system uses machine learning algorithms to find anomalies. It uses techniques like Isolation Forest, Support Vector Machine, CatBoost and LSTM Autoencoders to look at patterns in the data. These models are trained using benchmark datasets. Saved for later use. When the system is running the trained models are loaded to find anomalies in time. Using models helps find anomalies more accurately. The machine learning algorithms look at the output to see if the data is normal or not.If the machine learning algorithms find something is wrong they send out an alert. The machine learning algorithms give the attack a rating to show how bad the attack is so we know how serious the machine learning algorithms think the attack really is.

We use the rating, from the machine learning algorithms to understand what is going on with the attack and what the machine learning algorithms have found.When an anomaly is found the information is sent to the blockchain part of the system to be logged securely. The blockchain is set up using the Ethereum platform, where each anomaly event is recorded as a transaction. Cryptographic hashing techniques like SHA-256 are used to make sure the data is not changed. The blockchain provides a way to store data that's secure and cannot be changed.

To handle amounts of data the system uses decentralized storage with the InterPlanetary File System. Of storing all the data on the blockchain only a content hash is stored and the actual data is kept in the InterPlanetary File System. This way the system can handle data and store it more efficiently.

The backend of the system is set up using FastAPI, which allows for communication and supports asynchronous processing. The proposed solution makes it easy to work with the parts of the frontend machine learning and blockchain.

The proposed frontend is a website that you can use to see what is going on.It shows warnings about what the user's doing how the device is working and other things. The frontend lets users watch what is happening and make choices. The parts of the solution work together like a line of people doing a job.This line of people does things one after the other. These things include:Collecting data, Cleaning up the data,Using machine learning to look at the data and make decisions,Writing information on the blockchain, Showing the information, All these things happen on time.

The proposed solution finds out what is going on quickly and stores the data safely. The blockchain assisted anomaly detection framework, for securing IoHT devices is a thing.This framework uses blockchain to find out if something is wrong and keep IoHT devices safe.It makes sure that IoHT devices are safe.It does this by finding out what is happening and writing it down on the blockchain. The blockchain assisted anomaly detection framework is important.It keeps IoHT devices safe.The proposed solution works with this framework. They make sure that IoHT devices are safe and working properly.The proposed solution and the blockchain framework are necessary. They let users watch what is happening and make choices.The proposed solution and framework are necessary to keep IoHT devices safe.

VI. RESULTS AND DISCUSSION

The Blockchain-Assisted Anomaly Detection Framework for Securing IoHT Devices was tested to see if it really works. We wanted to know if it can find problems and strange things that happen and if it can secure the IoHT Devices.

The Blockchain-Assisted Anomaly Detection Framework for Securing IoHT Devices uses machine learning and blockchain technology together. It also has a dashboard that lets users see what is happening over time.When we tested the Blockchain-Assisted Anomaly Detection Framework for Securing IoHT Devices we did not get any warning messages.

This is good because it means the Blockchain-Assisted Anomaly Detection Framework for Securing IoHT Devices is working the way it should. It is doing its job. Meeting its goals.To start using the Blockchain-Assisted Anomaly Detection Framework for Securing IoHT Devices you need to log in.

You have to enter your user name and password. After you log in you can go to the webpage that has all the features you need. The Blockchain-Assisted Anomaly Detection Framework, for Securing IoHT Devices is pretty easy to use.

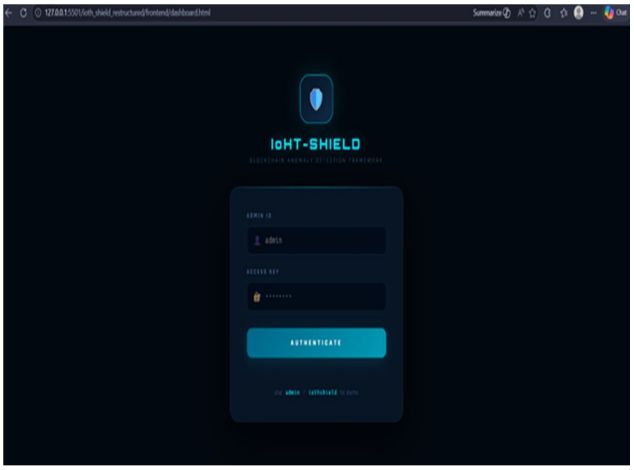


Fig. 2. User Login Interface

The home page shows us an overview of whats happening on the system.It tells us how many IoHT devices are working properly.It shows the number of anomalies that were detected.It also shows how well the models are doing at detecting things.In our test the Blockchain-Assisted Anomaly Detection Framework for Securing IoHT Devices really worked well.

It was able to spot anomalies.The home page told us that the models were 97% accurate.This was really impressive.The IoHT devices and models did a job of detecting anomalies.The home page is a place to get information on the IoHT devices and models.It helps us keep track of how everything's doing.The IoHT devices are doing well.The models are also performing well in detecting anomalies, on the IoHT devices.

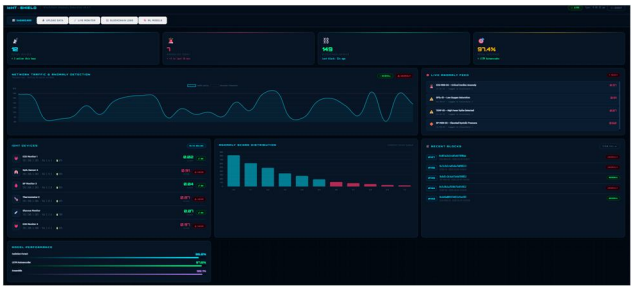


Fig. 3. Dashboard Overview

The Blockchain-Assisted Anomaly Detection Framework for Securing IoHT Devices has a part that watches the network. This part shows what the network traffic looks like and where problems start. If the traffic is too much it is considered suspicious. This helps us see if there are any issues.

There are two ways to find anomalies. The Blockchain-Assisted Anomaly Detection Framework for Securing IoHT Devices uses the Isolation Forest approach and the LSTM autoencoder. The Isolation Forest approach uses a tree-based algorithm to find outliers. It looks at data samples to see if they are similar or not. The Isolation Forest approach works with the Blockchain-Assisted Anomaly Detection Framework for Securing IoHT Devices when it comes to network traffic. Other people have used this approach before. It worked for them 90 to 96% of the time.

The LSTM Autoencoder is a model that finds anomalies by looking at data that changes over time and learning what is normal. It finds anomalies by rebuilding patterns. If it cannot rebuild a pattern the LSTM Autoencoder says it is an anomaly. The Blockchain-Assisted Anomaly Detection Framework for Securing IoHT Devices uses the LSTM Autoencoder model to find activity in sensors. The Blockchain-Assisted Anomaly Detection Framework for Securing IoHT Devices is good at finding problems in the network traffic and the Blockchain-Assisted Anomaly Detection Framework, for Securing IoHT Devices helps us evaluate the network.

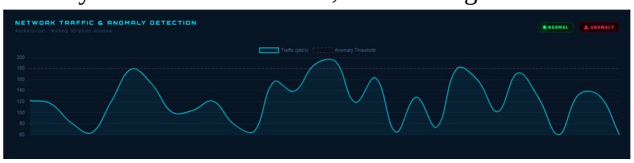


Figure 4. Anomaly Detection Graph

When we check the Blockchain technology for finding anomalies in IoHT devices we can see the status of these devices.Each IoT device shows how its working. If something is wrong it will show that too.The IoT devices will clearly show any information they have.We are looking at the Blockchain technology for IoHT devices.The Blockchain technology helps us find anomalies in IoHT devices.We focus on Blockchain, for IoHT devices.

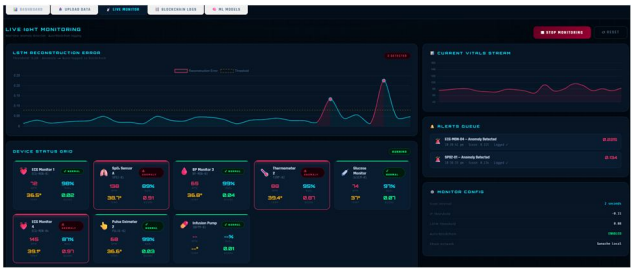


Fig. 5. Live IoHT Monitoring

It is worth noting that the Blockchain-Assisted Anomaly Detection Framework for Securing IoHT Devices performs exceptionally well in identifying anomalies within IoHT devices and generating alerts. The Blockchain-Assisted Anomaly Detection Framework for Securing IoHT Devices achieves the above through assessing the error that arises during reconstruction of the data using the LSTM autoencoder. In case the error exceeds the set threshold, the Blockchain-Assisted Anomaly Detection Framework for Securing IoHT Devices will automatically identify the anomaly within the system. It can be concluded that the use of Blockchain-Assisted Anomaly Detection Framework is very effective in handling the incoming data.

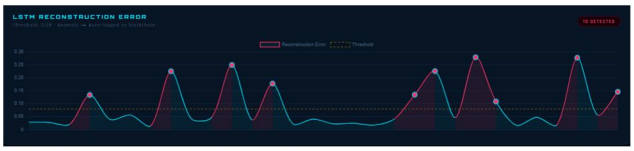


Fig. 6. LSTM Reconstruction Error

The anomaly score graph helps us see how the data points are grouped together based on the kind of anomalies they're The anomaly score graph is really useful for understanding anomalies in the data. Most of the data points are normal. They do not have any issues. There are a few data points that are not normal. These data points are called anomalies. In the part of the Blockchain-Assisted Anomaly Detection Framework for Securing IoHT Devices that uses Blockchain, the anomalies that are found are watched in blocks. Each block has the anomaly score and the time it was found and a special hash value. This helps us tell the difference between the anomalies and the normal data points.

It also helps keep the IoHT Devices secure. The Blockchain-Assisted Anomaly Detection Framework for Securing IoHT Devices is good at keeping the devices safe. The Blockchain-Assisted Anomaly Detection Framework uses blocks to watch for anomalies in the IoHT Devices. This is how the Blockchain-Assisted Anomaly Detection Framework keeps the devices safe from anomalies. The anomaly score graph and the blocks help us find the data points. We use the Blockchain-Assisted Anomaly Detection Framework to find the anomalies and keep the devices safe. The Blockchain-Assisted Anomaly Detection Framework is good, at securing the devices by watching for anomalies..

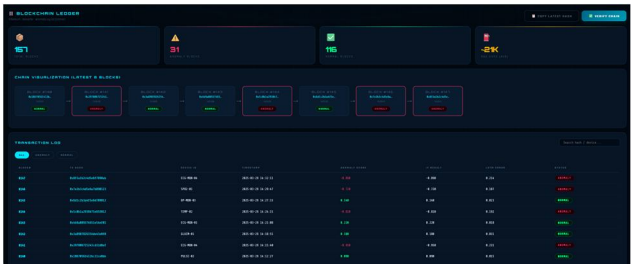


Fig. 7. Blockchain Logs

Therefore the Blockchain-Assisted Anomaly Detection Framework for IoHT Devices also has a feed that shows anomalies. This feed has data on anomalies happening now. It includes things like the name of the IoHT device. What the anomaly is.One way to see how well our models work is to look at how accurate they'reThe isolation forest model was 96% of the time.The LSTM autoencoder model was 97% of the time.However when we combined these two models the results were a bit better than the two models.In this case the Blockchain-Assisted Anomaly Detection Framework for IoHT Devices is what we are talking about.

The feed that shows anomalies in the Blockchain-Assisted Anomaly Detection Framework for IoHT Devices is very important.The Blockchain-Assisted Anomaly Detection Framework for IoHT Devices uses this feed to detect anomalies.The anomaly feed helps the Blockchain-Assisted Anomaly Detection Framework, for IoHT Devices work better.

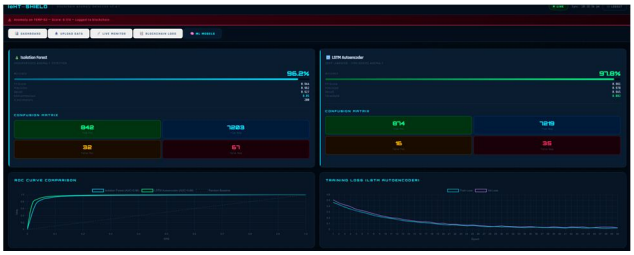


Fig. 8. Model Performance and Evaluation

The Blockchain Assisted Anomaly Detection Framework for IoHT Devices has a monitoring system.This system keeps track of events related to anomalies.It captures details like identifiers of IoHT devices, anomaly scores and timestamps.It also captures results from machine learning models. The system handles IoHT data streams in time and batch inputs efficiently.The experimental results show that it works well and reliably in detecting patterns.It combines machine learning and blockchain technology.This makes sure that anomaly detection is accurate and data is safe.

When an anomaly is detected the system records the event details on the blockchain. It stores data securely in IPFS.The results are displayed on a dashboard. This lets users monitor IoHT Device behavior and track anomalies.They can verify that data is authentic by checking blockchain records.This approach makes IoHT environments more trustworthy, transparent and secure.The Blockchain Assisted Anomaly Detection Framework for IoHT Devices is suitable for healthcare monitoring applications.The Blockchain Assisted Anomaly Detection Framework for IoHT Devices ensures that IoHT Devices are safe and secure.It does this by using blockchain and machine learning The Blockchain Assisted Anomaly Detection Framework for IoHT Devices keeps data secure.It helps in detecting anomalies in IoHT DevicesThe system is reliable and efficient.It works well in detecting patterns, in IoHT data streams..

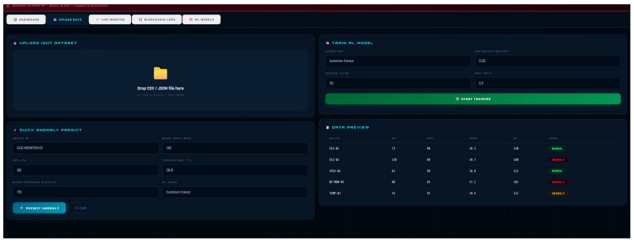


Fig. 9. Upload Dataset

VII. CONCLUSION

For the current paper, we have chosen IoHT-SHIELD technology as the topic of our study. "IoHT-SHIELD" stands for a methodology that utilizes the use of the blockchain approach and focuses on the detection of potential risks associated with the safety of IoT-H devices. It goes without saying that security concerns connected with the protection of IoT-H devices should never be ignored. Two points are crucial when it comes to securing IoT-H devices. Firstly, it is crucial to identify any threat. Secondly, it is vital to log all events associated with such threats safely. For the purpose of identifying threats to the IoT-H device, the approach of IoHT-SHIELD technology utilizes various machine learning techniques such as Isolation Forest and SVM, CatBoost and LSTM Autoencoders. Blockchain approach in IoT-H devices uses the technologies of Ethereum blockchain and IPFS respectively.People tested IoHT-SHIELD. It worked well. It found threats accurately. It kept events safe. This is important for healthcare because healthcare has a lot of rules. IoHT-SHIELD is also flexible. It can work with many different Internet of Healthcare Things devices. It can process data in time and it keeps a clear record of what happens.

In the future, our efforts will focus on improving IoHT-SHIELD by adding features that clarify its functionality. These updates will include testing with device data, incorporating various sensor data types, and optimising the blockchain component for faster performance.The primary aim of IoHT-SHIELD is to protect IoHT devices, which it accomplishes by detecting devices and maintaining secure records. This enables early threat detection and keeps device data secure. The system is valuable for monitoring IoHT devices, analysing data, and ensuring their proper operation. Overall, IoHT-SHIELD is essential for maintaining the security of IoHT devices.

VIII. FUTURE WORK

IoHT-SHIELD is a working prototype, but like any first version, it leaves room to grow. The five directions below are where we think the most meaningful improvements can be made.

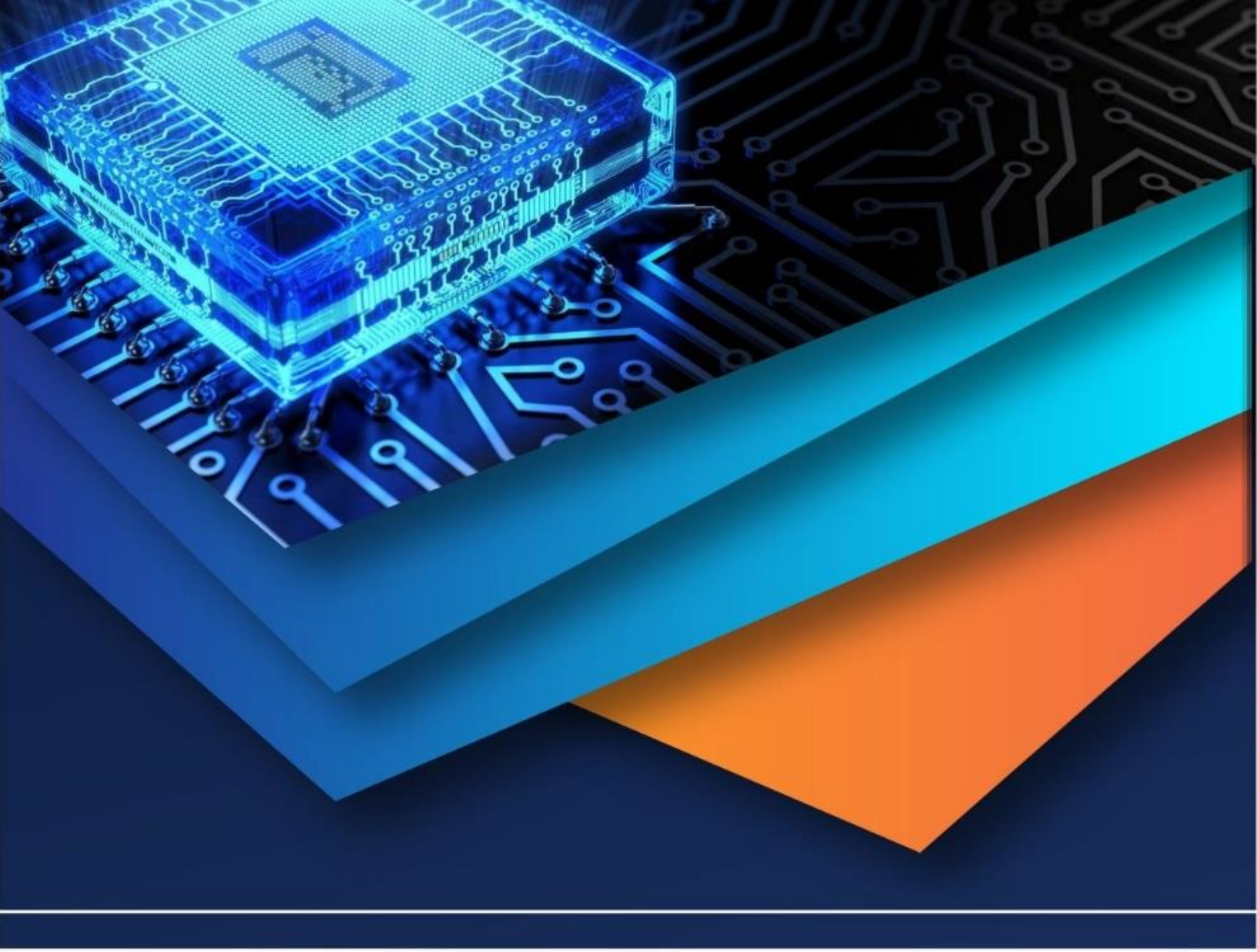
The one limitation we noticed most during development is that the system can tell you *that* something went wrong, but not *why*. Isolation Forest and the LSTM Autoencoder produce scores, not explanations. For a nurse or a biomedical engineer reviewing an alert, that distinction matters. Adding SHAP-based attribution or attention heatmaps would let users trace a flagged event back to the specific sensor readings or time intervals that caused it — making the system something people can actually reason about, not just react to.

The second issue is that everything so far has been tested on datasets, not real hardware. Benchmark data is clean and well-structured in ways that real IoHT deployments simply are not. Wearables drop readings. Network conditions fluctuate. Device firmware varies across manufacturers. Until IoHT-SHIELD is validated against live streams from actual devices, its real-world performance remains an open question. That validation is the logical next step.

There is also an opportunity to broaden what the system pays attention to. Right now, anomaly detection operates primarily on device telemetry. But security-relevant behavior often shows up in adjacent signals — unusual network traffic, environmental changes, or shifts in how a patient is moving. Feeding those additional channels into the detection pipeline should make it harder for subtle attacks to go unnoticed, since an adversary would need to simultaneously manipulate multiple data streams to evade detection.
The blockchain layer works, but it was not designed with throughput as the primary constraint. At scale, per-transaction gas costs and confirmation delays could become a real operational problem. Batching anomaly records through a layer-two solution, or switching to a lighter consensus protocol for the logging function, would reduce that overhead without sacrificing the tamper-evidence property that makes the blockchain useful in the first place.
Lastly, the current training approach assumes that data can be aggregated centrally — which is a reasonable assumption for a prototype but a problematic one for a system deployed across multiple hospitals or clinics. Federated learning would allow each site to improve the shared model using its own patient data without that data ever leaving the local network. It is a natural fit for healthcare, and it would make IoHT-SHIELD significantly more practical to deploy at scale.
None of these are small tasks, but each one addresses a concrete limitation in the current system. The goal is a framework that works not just on paper, but in the middle of a clinical environment where reliability is not optional.

REFERENCES

[1] M. Islam, A. S. Dukyil, S. Alyahya, and S. Habib, “An IoT Enabled Anomaly Detection System for Smart City Surveillance using 2D-CNN and Echo State Networks,” Sensors, vol. 23, no. 4, 2023. [Online]. Available: https://www.mdpi.com/1424-8220/23/4/2358
[2] K. DeMedeiros, A. Hendawi, and M. Alvarez, “A Survey of AI-Based Anomaly Detection in IoT and Sensor Networks,” Sensors, vol. 23, no. 3, 2023. [Online]. Available: https://www.mdpi.com/1424-8220/23/3/1352
[3] A. Chatterjee and B. Ahmed, “IoT Anomaly Detection Methods and Applications: A Survey,” arXiv preprint, 2022. [Online]. Available: https://arxiv.org/abs/2207.09092
[4] M. I. H. Okfie et al., “Anomaly Detection in IIoT Transactions using Machine Learning and Blockchain,” Engineering, Technology & Applied Science Research, 2024. [Online]. Available: https://www.etasr.com/index.php/ETASR/article/view/7384
[5] “A Survey of Anomaly Detection in IoT Networks Using Machine Learning,” International Journal of Creative Research Thoughts (IJCRT), 2024. [Online]. Available: https://www.ijcrt.org/papers/IJCRT2402509.pdf
[6] M. Domb, “Anomaly Detection in IoT: Recent Advances, AI and ML Techniques,” IntechOpen, 2023. [Online]. Available: https://www.intechopen.com/chapters/87783
[7] M. M. Khan et al., “Anomaly Detection in IoT-Based Healthcare Using Machine Learning,” PubMed, 2024. [Online]. Available: https://pubmed.ncbi.nlm.nih.gov/38467709/
[8] J. Jot and L. S. Sharma, “Anomaly Detection in IoT Sensors using Machine Learning,” IJRASET, 2023. [Online]. Available: https://doi.org/10.22214/ijraset.2023.55226
[9] H. Zahan et al., “IoT-AD: A Framework to Detect Anomalies Among Interconnected IoT Devices,” arXiv preprint, 2023. [Online]. Available: https://arxiv.org/abs/2306.06764
[10] T. Lai et al., “Ensemble Learning based Anomaly Detection for IoT Cybersecurity,” arXiv preprint, 2023. [Online]. Available: https://arxiv.org/abs/2307.10596



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY