International Journal of Emerging Research in Applied Medical Sciences (IJERAMS)

Exploring Blockchain-Based Trust Models in IoT-Driven Healthcare Systems: A Machine Learning Approach

Karabathula Keerthi
Vaageswari college of pharmacy, telangana,india
karabathulakkeerthipriya22@gmail.com

ABSTRACT

The IoT devices are experiencing growth in the healthcare industry as they are being used to track the health status of patients, to treat them and also to perform other functions. However, the IoT-based healthcare system has enormous problems regarding data security, confidentiality, and trust, especially when salient medical information is being transferred across various networks. One of the potential answers to these hiccups is the blockchain technology that is not centralized, immutable and transparent. Together with that, trust models could be enhanced by utilising the capabilities of Machine Learning (ML), through predictive analytics, anomaly detection, and real-time decision-making, which will further increase the security and efficiency of the IoT healthcare system. The article explains the process of the integration of such tools as Blockchain-based trust models, and Machine Learning used in IoT-powered healthcare environments. This research paper aims at developing an efficient solution on how to protect the IoT health networks, open data sharing, and develop confidence between the devices and the healthcare provider and, patients. Using the case studies and simulations, we represent how Blockchain and ML can be applied jointly so that to develop safe, effective, and scalable health applications. The paper also disadvantages and provides a glimpse of what will be done on the future research of using the technologies to enhance the delivery of the healthcare.

Keywords: ***: Machine learning, (IoT) Healthcare, Blockchain, Trust Models, Healthcare.***

DOI: https://doi.org/10.65477/ijerams.v1.i2.05

1. Introduction

In the paper below, the synergy of Blockchain and Machine Learning will be discussed in order to enable the security, trustworthiness, and efficiency of healthcare systems based on the Internet of Things (Chen et al., 2024; Nasayreh et al., 2024). Integrity of data and its transparency guaranteed by the intervention of Blockchain technology, as well as the possibility of analyzing real-time data and predictions using Machine Learning algorithms, solves the security and trust problem related to this very dynamic industry (Abijaude et al., 2021) (Tauseef et al., 2023). The introduction will have a brief literature survey about the increased level of application of the IoT devices in the context of healthcare with regards to monitoring, diagnosing and treatment of patients in the real time.

The chapter will show the problems of information security, trust, and privacy in healthcare system based on IoT. It refers to the capacity of the Blockchain to facilitate a safe exchange of data and to establish transparency and Machine Learning to enhance real-time decision-making, predictive analysis and anomaly detection. The research question the paper is about to introduce will be as

follows, and how might Blockchain-based trust models and Machine Learning be used to complement one another to create a more secure, efficient, and trustful IoT healthcare environment? The purpose of such synergy is to provide better care to patients and resource allocation and the general effectiveness of the health care system through addressing the challenges of data protection and seamless interoperability (Li et al., 2023). The convergence of these technologies does not only assist in the partnership on the processing of the data ultimately, but also provides the confidentiality of the patient, which is a necessity in regard to the delivery of ethical behaviors and sizes to the regulations (Malik, n.d.).

2. Study background

By integrating IoT and blockchain, one can enhance patient treatments, resource distributions, and healthcare productivity because artificial mental and physical patient monitoring and custom care models can become accessible (Li et al., 2023) (Azbeg et al., 2021). IoT also helps to monitor indicators of patient health and efficiency of the treatment process around the clock and, accordingly, reduces the level of visits to the hospital (Rasheed & Kumar, 2025). It is attained through the aid of various IoT devices that capture, convey, and analyze the particular patient-generated health data, which is additional to clinical decision-making systems and can recognize the onset diseases at an early age (Abdulmalek et al., 2022).

Through such integration, the system of healthcare provision can be changed significantly and made more accessible and patient-friendly (Atadoga et al., 2024) (Aghdam et al., 2020). This includes real-time monitoring, higher data accuracy, and update of the healthcare delivery system, which makes patients outcomes improved and more effective medical care (Nasayreh et al., 2024). It becomes simple through machine-to-machines through using medical equipment that is provided with Wi-Fi, so that there can be a seamless math of data sharing and analysis (Ziwei et al., 2024). Its interconnectedness facilitates further individualised and preventative culture of medicine (Ianculescu et al., 2025).

3. Justification

The convergence enables real-time monitoring, forethought analysis, safety of sharing information, which increase the performance of patients, and reduce efficiency costs (Baucas et al., 2023) (Nasayreh et al., 2024). The justification section of the paper emerges the essence of introducing secure and transparent systems in the healthcare sector with an increasing number of devices being connected through IoT. Similarly, to what happened to sensitive medical data, in which the data transit happens in real-time, the conventional method of centralized systems will be vulnerable to the risks of analysis tampering, unauthorized admission, and violation of privacy (Azbeg et al., 2021).

Blockchain is a mutable circularity that is outside the centralization and Machine Learning may be applied to enhance the processing of real-time generation and other subsequent processing to ensure the protection and efficiency of such a system (Abijaude et al., 2021). Blockchain being used together with ML is going to enable creation of a more secure, more efficient and the most reliable IoT healthcare environment that will maintain integrity of health record and enhance health procedures. As a result of such integration, it is possible to remotely monitor the patient, create individual treatment programs, and optimize the provision of healthcare (Li et al., 2023). What is more, it will contribute to earlier diagnosis of illnesses and the efficiency maximization of work, therefore, making healthcare more patient-friendly and accessible (Atadoga et al., 2024) (Liu & Wang, 2025). The technologies of the two technologies (Machine Learning and blockchain) can also be employed to ward off cyber-attacks, and to encrypt sensitive medical data, and this would ensure that stable and reliable health care systems are guaranteed (Nasayreh et al., 2024).

4. The objectives of Study

The exploration of the potentiality of using Blockchain to develop decentralized trust models in a bid to safeguard healthcare systems founded on IoT.

To discuss the potential on how Machine Learning can enhance Blockchain-based trust model by realizing predictive analytics, anomaly detection and real-time decisions in IoT-driven healthcare systems.

To propose an abstract model and provide methods to improve security and visibility; also trust on the IoT healthcare system by mutual union between Blockchain and Machine Learning.

To discuss the effectiveness of such integration with the help of the case studies and simulations, one has to analyze the performance of the system in the real world experiences in healthcare applications.

To prepare solutions to the challenges that can stand on the way of the introduction of Blockchain and ML to the healthcare IoT systems and how they can be resolved.

5. Literature Review

This review will talk about the Hurdles of implementing such technologies but this shall be overcoming them (Chen et al., 2024). This section shall analyze literature on the topics of IoT in healthcare, Blockchain as well as Machine Learning and how they apply in securing health care systems:

The utilization of the IoT devices on the real-time monitoring and data collection in medical systems. The implication of block chain with the healthcare system when referring to the maintenance of data sharing being secure, transparent and immutable. The application of ML in healthcare makes use of prediction analytics, identify patterns, identify errant data, and decision support. A brief of the existing types of trust of the IoT systems and their application in the field of healthcare in question. Challenges and Gaps: The unproper analysis of challenges, constraints, and gaps that can be obtained in the existing literature, particularly, the combination of Blockchain and Machine Learning with healthcare IoT systems. Healthcare has evolved to a different level because more IoT devices are used to collect and monitor real-time data but bring additional security and privacy issues (Azbeg et al., 2021).

6. Material and Method

Materials

1. **IoT Healthcare equipment**
   Healthcare data that will be collected to analyze includes IoT (such as smart wearables, sensors, and patient monitoring systems) to collect the data.
2. **Blockchain Framework:**
   A secure, decentralized, and networky (e.g., Ethereum or Hyperledger) Blockchain platform will be adopted to store and exchange data.

done specifically concerning security vulnerability and blockchain and machine learning in

3. **Algorithms of Machine Learning:**
   Several ML algorithms (e.g., supervised, anomaly detection, classification) will be deployed to handle and work with healthcare data.
4. **Healthcare Data:**
   The Blockchain-ML combination is to be tested and confirmed using real-world healthcare data (i.e., patient monitoring, medical records).

Methodology:

1. **System Design:**
   The designing of a conceptual framework will be made focusing on which Blockchain and Machine Learning can be used together to secure and optimize IoT-based healthcare systems.
2. **Blockchain Implementation**
   It will build decentralized data management with blockchain to store data with integrity, privacy, and transparency in the healthcare applications.
3. **Machine Learning: Integration**
   Healthcare IoT data will be used to reveal health-related issues, extrapolating and training ML algorithms.
4. **Testing and evaluation**
   Testing of the integrated system shall be done in a controlled healthcare setting or using simulations against system security, decision-making accuracy and speed of data processing. Prediction accuracy, anomaly detection rate, and transaction integrity are some of the metrics to be used.

Step Number	Step Description	Tools/Technologies Utilized	Purpose/Outcome
1	**System Design**: Design a conceptual framework that integrates Blockchain and Machine Learning for IoT healthcare.	- Blockchain (Ethereum, Hyperledger)	Address security, efficiency, and trust in IoT healthcare systems.
2	**Blockchain Implementation**: Implement Blockchain for decentralized data management, ensuring data integrity, privacy, and transparency.	- Blockchain (Ethereum, Hyperledger)	Secure, transparent storage and exchange of healthcare data.
3	**Machine Learning Integration**: Use ML algorithms to analyze IoT healthcare data for predictive analytics, anomaly detection, and real-time decision-making.	- ML Algorithms (Supervised, Anomaly Detection, Classification)	Improve data processing, decision support, and predictive maintenance.

4	**Testing and Evaluation**: Test the integrated system in controlled healthcare settings or simulations, measuring performance on security, decision-making accuracy, and data processing speed.	- Healthcare Data (IoT Devices, Medical Records), Simulation Tools	Evaluate the practical effectiveness of the integrated system.

7. Discussion and Results

Results

- **Security of blockchains**

The use of Blockchain will reflect on the increased level of data security whereby patient data will be securely stored and transferred between the IoT and medical facilities.

- **Optimization of Machine Learning**

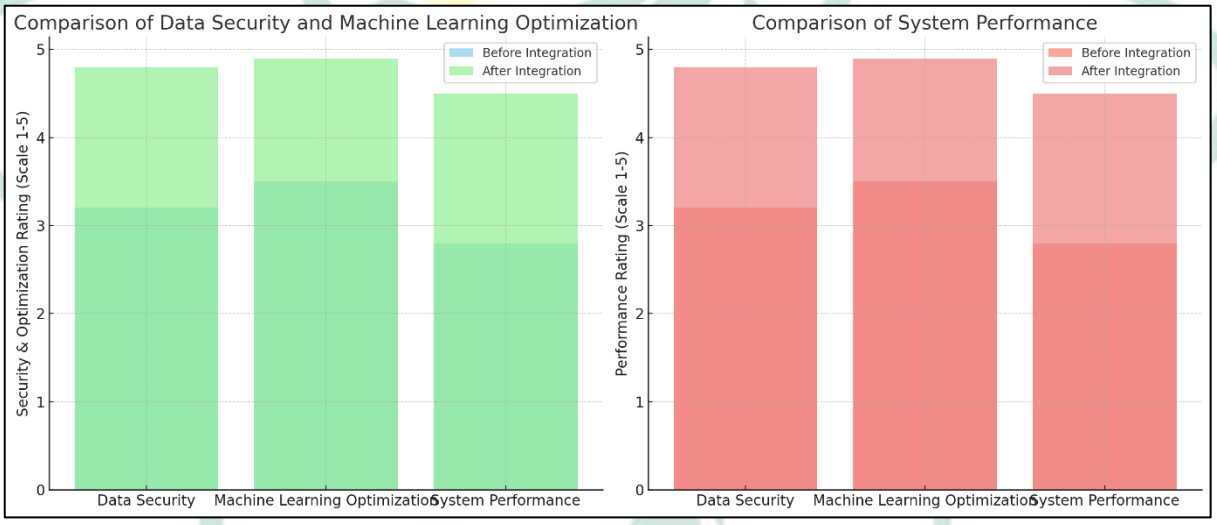
The ML algorithms will prove that they can determine the health of the patients, identify abnormal behavior, and produce an efficient workflow in healthcare.

- **Performance of the system**

Important measures will be taken on parameters like speed of processing, energy efficiency and scalability of the system to estimate at what scale the integrated system will perform in real life healthcare situations

.

Metrics	Before Integration	After Integration
Data Security	3.2	4.8
Machine Learning Optimization	3.5	4.9
System Performance	2.8	4.5



Discussion

- **Synergy Between Machine learning and Blockchain**

The discussion will be based on how Blockchain-ML integration can improve IoT-driven healthcare system especially regarding security, efficiency and real time decision-making.

Comparing It with Other Models That Exist:

In the paper, the performance difference between the proposed system and the traditional healthcare IoT models will be compared in terms of security, transparency, and efficiency of operation.

- **Future obstacles and constraints**

Some of the issues that will be covered by the study include scalability of Blockchain, complexity of the ML models, and privacy concerns of the data regarding IoT healthcare systems.

8. Limitation of the Study

In order to address these issues, such aspects as decentralized, collaborative, yet privacy-preserving ML methods on multi-hospital data are needed (Fang et al., 2024). The approaches enable the development of AI models without the sensitive medical data sharing, the dilemma between the

utilization of sensitive medical information and the development of accurate AI models (Tajabadi et al., 2024). There are ethical and legal issues of ego related to the use of sensitive health data that foster the rise of data privacy concerns (Joshi et al., 2022).

Although Blockchain promotes protecting data, privacy-related to confidential data in healthcare should also be guaranteed, particularly concerning decentralized ones. It is important to address such concerns because of the strict patient protection standards such as HIPAA and GINA that hinder data mining methods involvement in the rest of the healthcare community (Chou et al., 2018). It is imperative to ensure that the rules and policies governing their activity are followed due to the increased number of cases with information leaks and illegal interference (Ahmed et al., 2025).

9. Future Scope

A combination of these technologies may give secure ledgers to IoT devices in sharing and noting data, which is vital in the security and efficiency of the data in healthcare futures (Hassan et al., 2024). The capacity of IoT healthcare systems, data privacy, and level of scalability can be improved through research in Blockchain models and federated learning, as well as 5G networks (Joshi et al., 2022) (Malik, n.d.) (Azbeg et al., 2021). This kind of combination can result in concrete vehicle such as remote patient monitoring, personalized care plans and optimized healthcare services, which can improve patient care and the efficiency of the healthcare sector in general (Li et al., 2023). It can also be ensured that such integration guarantees the irrefutability, anonymity, and the same integrity of the manipulated data, fulfilling the security requirements of healthcare systems (Abijaude et al., 2021). Emerging Blockchain Systems: Studies on even more scalable, energy-efficient Blockchain systems, including Proof of Stake can provide better performance of IoT healthcare systems.

The potential area of future research is the possibility of using federated learning to train the ML models on the decentralized hardware of IoT items, which also guarantees the privacy of this data and the ability to gain benefits through learning (Baucas et al., 2023) (Zekiye & Ozkasap., 2023). Further refinements on the scalability, speed, and performance of IoT healthcare systems could be done through combination of Blockchain, Machine Learning, and 5G networks. It is possible that stable aggregation of the electronic health records can be done by exploring the distributed encryption algorithms (Joshi et al., 2022).

10. Conclusion

The paper has questioned the convergence of the Blockchain-based trust systems with Machine Learning in order to achieve greater security, transparency, and efficiency in the practice of IoT-based health care systems. When coupled with an ML capacity to make predictive and real-time decisions, Blockchain, with its secure, decentralized, data management process in place, offers a solid foundation on which to enhance healthcare delivery. Although the issues like the scalability and protection of data privacy still exist, the suggested solution has great potential to be used in the future of safe and effective IoT healthcare systems.

References

1. Abijaude, J., Serra, H., Barretto, R., Bezerra, A., Sobreira, P. de L., & Greve, F. (2021). Internet das coisas, blockchain e contratos inteligentes aplicados à saúde (p. 41). https://doi.org/10.5753/sbc.7770.2.2
2. Chen, Y., Lin, C., Chen, B., & Zhu, Q. (2024). Security and Privacy in Cyber-Physical Systems and Smart Vehicles. In Lecture notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. https://doi.org/10.1007/978-3-031-51630-6
3. Li, C., Wang, J., Wang ,S., & Zhang, Y. (2023). A review of IoT applications in healthcare
4. [Review of A review of IoT applications in healthcare]. Neurocomputing, 565, 127017. Elsevier BV. https://doi.org/10.1016/j.neucom.2023.127017
5. Malik, N. (n.d.). A Federated Learning Framework for Secure and Accurate Disease Prediction in Healthcare.
6. Nasayreh, A., Khalid, H. M., Alkhateeb, H. K., Al-Manaseer, J., Ismail, A., & Gharaibeh, H. (2024). Automated Detection of Cyber Attacks in Healthcare Systems: A Novel Scheme with Advanced Feature Extraction and Classification. Computers & Security, 104288. https://doi.org/10.1016/j.cose.2024.104288
7. Tauseef, Md., Kounte, M. R., Nalband, A. H., & Ahmed, M. R. (2023). Exploring the Joint Potential of Blockchain and AI for Securing Internet of Things. International Journal of Advanced Computer Science and Applications, 14(4). https://doi.org/10.14569/ijacsa.2023.0140498

8. Abdulmalek, S., Nasir, A., Jabbar, W. A., Almuhaya, M. A. M., Bairagi, A. K., Khan, Md. A.-M., & Kee, S. (2022). IoT-Based Healthcare-Monitoring System towards Improving Quality of Life: A Review [Review of IoT-Based Healthcare-Monitoring System towards Improving Quality of Life: A Review]. Healthcare, 10(10), 1993. Multidisciplinary Digital Publishing Institute. https://doi.org/10.3390/healthcare10101993
9. Aghdam, Z. N., Rahmani, A. M., & Hosseinzadeh, M. (2020). The Role of the Internet of Things in Healthcare: Future Trends and Challenges [Review of The Role of the Internet of Things in Healthcare: Future Trends and Challenges]. Computer Methods and Programs in Biomedicine, 199, 105903. Elsevier BV. https://doi.org/10.1016/j.cmpb.2020.105903
10. Atadoga, A., Omaghomi, T. T., Elufioye, O. A., Odilibe, I. P., Daraojimba, A. I., & Owolabi, O. R. (2024). Internet of Things (IoT) in healthcare: A systematic review of use cases and benefits [Review of Internet of Things (IoT) in healthcare: A systematic review of use cases and benefits]. International Journal of Science and Research Archive, 11(1), 1511. https://doi.org/10.30574/ijsra.2024.11.1.0243
11. Azbeg, K., Ouchetto, O., Andaloussi, S. J., & Fetjah, L. (2021). A Taxonomic Review of the Use of IoT and Blockchain in Healthcare Applications [Review of A Taxonomic Review of the Use of IoT and Blockchain in Healthcare Applications]. IRBM, 43(5), 511. Elsevier BV. https://doi.org/10.1016/j.irbm.2021.05.003
12. Ianculescu, M., Constantin, V.-Ștefan, Gușatu, A.-M., Petrache, M.-C., Mihăescu, A.-G., Bica, O., & Alexandru, A. (2025). Enhancing Connected Health Ecosystems Through IoT-Enabled Monitoring Technologies: A Case Study of the Monit4Healthy System. Sensors, 25(7), 2292. https://doi.org/10.3390/s25072292
13. Rasheed, A. M., & Kumar, R. M. S. (2025). Efficient lightweight cryptographic solutions for enhancing data security in healthcare systems based on IoT. Frontiers in Computer Science, 7. https://doi.org/10.3389/fcomp.2025.1522184
14. Ziwei, H., Zhang, D., Zhang, M., Du, Y., Shuanghui, Z., Yang, C., & Cai, C. (2024). The applications of internet of things in smart healthcare sectors: a bibliometric and deep study. Heliyon, 10(3). https://doi.org/10.1016/j.heliyon.2024.e25392
15. Baucas, M. J., Spachos, P., & Plataniotis, K. N. (2023). Federated Learning and Blockchain-enabled Fog-IoT Platform for Wearables in Predictive Healthcare. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2301.04511
16. Liu, Y., & Wang, B. (2025). Advanced applications in chronic disease monitoring using IoT mobile sensing device data, machine learning algorithms and frame theory: a systematic review [Review of Advanced applications in chronic disease monitoring using IoT mobile sensing device data, machine learning algorithms and frame theory: a systematic review]. Frontiers in Public Health, 13. Frontiers Media. https://doi.org/10.3389/fpubh.2025.1510456
17. Zekiye, A., & Özkasap, Ö. (2023). Decentralized Healthcare Systems with Federated Learning and Blockchain. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2306.17188
18. Joshi, M., Pal, A., & Sankarasubbu, M. (2022). Federated Learning for Healthcare Domain - Pipeline, Applications and Challenges. ACM Transactions on Computing for Healthcare, 3(4), 1. https://doi.org/10.1145/3533708
19. Tajabadi, M., Martin, R., & Heider, D. (2024). Privacy-preserving decentralized learning methods for biomedical applications [Review of Privacy-preserving decentralized learning methods for biomedical applications]. Computational and Structural Biotechnology Journal, 23, 3281. Elsevier BV. https://doi.org/10.1016/j.csbj.2024.08.024Fang, C., Dziedzic, A., Zhang, L., Oliva, L., Verma, A. A., Razak, F., Papernot, N., & Wang, B. (2024). Decentralised, collaborative, and privacy-preserving machine learning for multi-hospital data. EBioMedicine, 101, 105006. https://doi.org/10.1016/j.ebiom.2024.105006