Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 6, 2026

INTEGRATION OF MACHINE LEARNING WITH BLOCKCHAIN FOR HEALTHCARE SYSTEM

Salma Rasool[*1], Shoaib Hassan[2], Unzila Nasir[3], Khadija Mumtaz[4], Hamza Bashir[5], Ayesha Siddiqa[6]

[*1,2,3,4,5,6]*Dept. Computer Science, The University of Lahore, Sargodha Campus, Sargodha, Pakistan*

[*1]70159409@student.uol.edu.pk, [2]shoaibcomsats11@yahoo.com, [3]70183292@student.uol.edu.pk, [4]70183294@student.uol.edu.pk, [5]70192947@student.uol.edu.pk, [6]70183422@student.uol.edu.pk

DOI: https://doi.org/10.5281/zenodo.20591131

Keywords
Blockchain, IOT, Machine Learning Healthcare system

Article History
Received: 09 April 2026
Accepted: 21 May 2026
Published: 08 June 2026

Corresponding Author: *
Salma Rasool

Abstract

The developments that took place in the fields of Blockchain Technology, Internet of Things (IoT), and Machine Learning (ML) offer promising and exciting developments within the paradigm shift that took place within various sectors, especially within the health industry. The intersection of these three will address issues on data security and privacy within the context of real-time decision-making. Within this research study, the intersection of IoMT and Blockchain technologies will be explored within the context of how the implementation of Blockchain Technology supports a secure data transfer process within a decentralized IoT environment. Second is the Federated Learning (FL) within the context of ML and its role within the privacy of ML. We analyze 16 recent papers that combine the use of Blockchain, IoT, and ML models, especially for applica- tions in the areas relating to healthcare, security, and others associated with 6G communication technologies. The papers show that the application of Blockchain technology enhances the management of healthcare data from the IoT, while ML models using healthcare datasets from the IoT improve real- time healthcare analysis and anomaly identification.Moreover, the combination of FL with Blockchain technology provides a secure framework for collaborative learning among devices using IoT technology. However, despite the vast potential benefits, there are also challenges in the realm of scalability, computational complexity, privacy concerns in relation to the use of data, and a lack of legal framework regulation that currently hinder the broader adoption of these combined platforms. This article will offer a broad review on the present status of related research experiments and advance future directions related to the ability of 6G communications to help provide a seamless combination of these concepts for the development of intelligent, safe, and optimized IoT platforms.

I. INTRODUCTION

With the integration of Blockchain, IoT and AI4, from the time being, in many use-cases can already be seen such complete, efficient intelligent systems of systems. This kind of healthcare system should extend also to, notably, healthcare wearables. The Internet of Medical Things (IoMT) helps us now to carry on modern medicine without going outside of philosophy by giving doctors a perspective in which they see Identify applicable funding agency here. If none, delete this. everything synchronously as if from

one comprehensive side out of many sides. Health information can be shared across systems instantly to boost its effect. Yet the potential rush of SiMT seems to be checked by the simple fact that health- care data is spread out. This is a nightmare for all medical consumers worried over both their privacy and confidentiality. Blockchain, in the same way, has proven indispensable in solving these cancers because its decentralized, trusted and permanent chain can disappear into any available format format free from requirements by anyone else.

While AI and models work together to enable intelligent decision-making, blockchain ensures the security of IOT de- vices. Predictive analytics is made possible by the large data storage capacity of IOT devices and machine learning models. These models can be used to identify deviations, improve resource distribution, and use customised infrastructures to address users' health needs. Federated Learning (FL), a decen- tralised machine learning technique where models are trained on data stored across various IOT devices without violating data privacy, is also supported by AI, much like Blockchain. In light of the numerous current interfaces with nearby medical facilities that are starting to edge internet wards for patient data transmission, this paper focusses on the interconnection of Blockchain, IOT, and AI in healthcare.It also speculates on how such trends might affect both 6G 's nature awesome so demands for medicine in future times.

II. LITERATURE REVIEW

A. Blockchain and IoT in Healthcare

Recently, the idea of bringing technology into health care systems using block chains has attracted much attention in China. This is seen as an authentic solution below for security and decentralized maintenance of sensitive patient data. The MoH cautioned against the current dispersed state of the country's health information – obviously it can be a threat to protect personal privacy. Those given office to safeguard their rights by that department may take for granted how they are ignored and infringed in every conceivable way: someone comes along at night, peering into things popping things in, and fifty varieties of people are having a go at the sources. Now if blockchains, that distribute data and will only write once mode are the future of secure transfer and storage of said data, how far have we come on good old privacy, security and trust front? For example, Ali et al. (2025) consider the role of blockchain technology within IoMT that might provide a secure, transparent and traceable verification and management of medical data. Moreover, Akrami et al. (2023) focus on the importance of blockchain in achieving secure data transmission between patients and healthcare providers within distributed healthcare systems where patients own and manage their medical records.

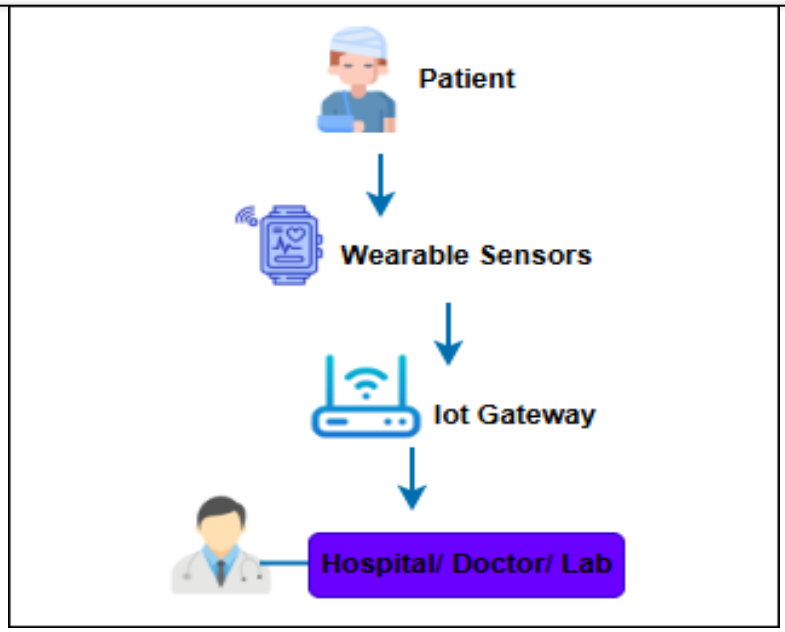

Fig. 1. Blockchain and IoT in Healthcare

This image visualizes how a health monitoring IoT system works. It starts from the patient side: the patient puts on a device under her clothing (it could be, for example, a smartwatch or a medical band). Unni and his team are working on a prototype of a wristband computer that can measure a user's heart rate, body temperature and blood pressure. The data is sent to an IoT gateway that intermediately connects and forwards the obtained values in a secure way to health care systems. The data is then sent to the hospital, doctor's clinic or at the medical lab where health care providers analyze and take real-time decisions on patients' eventual condition.

B. Federated Learning (FL) and Blockchain Integration

Federated Learning (FL) is a novel approach that enables fully decentralized learning among devices and servers while preventing users from sharing their private data with each other. As a result, an FL-based system can achieve global model convergence while maintaining data privacy. By training models directly on IoT-generated data, FL reduces the privacy risks associated with centralizing sensitive medical informa- tion. To the best of our knowledge, no existing machine learning framework fully exploits both privacy-preserving mechanisms and data immutability provided by blockchain technology. This integration also prevents malicious data from being injected into the model training process. Moreover, XYZ et al. (2017) demonstrate that combining FL with blockchain can certify training data as secure, predictable, and traceable. This trade-off is particularly attractive for sensitive medical applications. Similarly, Kuznetsov et al. (2024) investigate the use of blockchain to enable resilient training of decentral- ized machine learning models, focusing on weak healthcare systems. Their approach facilitates the development of AI models that are more trustworthy and transparent. Alghamedy et al. (2024) further show that integrating FL with blockchain ensures that training data are secure, authentic, and verifiable, which is especially important for privacy-sensitive domains such as healthcare.

C. AI and IoT Integration for Smart Healthcare

24ML and AI enabled real-time IoT data analysis have dramatically elevating the bar of healthcare applications. These use cases depend on the uninterrupted flow of data originated in IoT device systems. New electronic health generation

technologies that capture and analyze patient vitals with the ability to infuse predictive analytics and personalized clinical care planning—to a far more dynamic, proactive level than we have been able to do up to this point. Alghamedy et al. (2024) emphasize this improvement and the need to guarantee patient´s access to quality care.

Ali et al. (2025) also indicated that AI is advancing in-situ healthcare through amalgamating the IoT data with blockchain. Their work is concentrating on early disease detection and a real-time warning system, which can allow for better decision-making when planning interventions. By analyzing data from wearable devices, sensors, and other IoT tools, AI models enable medical staff to make more accurate and timely clinical decisions. Such an approach delivers personalized healthcare services that are aligned with individual patient needs.

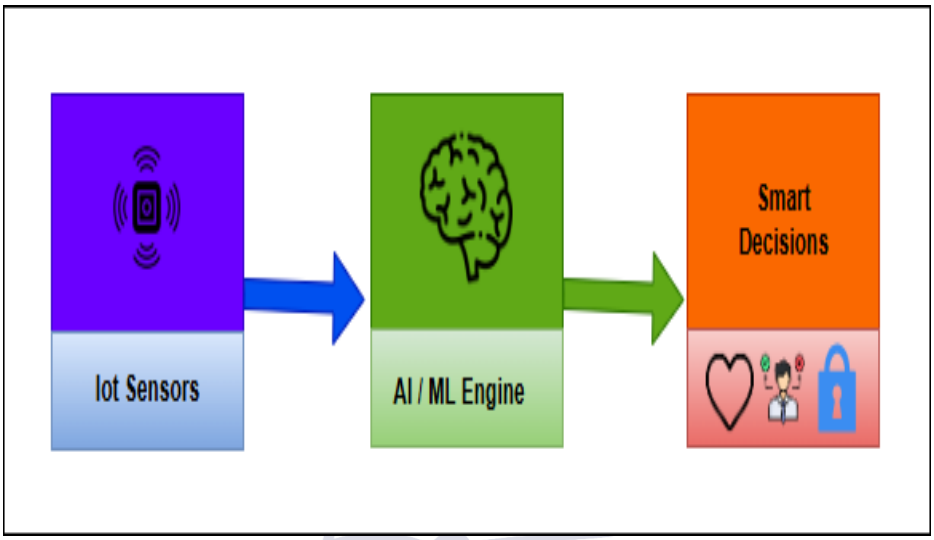

Fig. 2. AI and IoT Integration for Smart Healthcare

IoT sensors help to acquire real-time health data from the patient and transmit this data to an AI and ML engine. The AI engine processes and analyzes the data to identify abnor- malities and health hazards. According to the analysis, the engine helps to create intelligent decisions like notifications, recommendations, and/or diagnosis.

D. AI-Driven Decision Making in Healthcare

However, as an example, for any disease category, AI- related molecular testing is blooming. On top of that, and alongside other diagnostic assistants, it has transformed doc- tors into personal medicine planners, or at least decision-based medical guild members with higher technical skills mixed in. Alghamedy et al. (2024) discuss the future of AI and federated learning, highlighting safe, privacy-preserving, and efficient collaborative learning for healthcare. Akrami et al. (2023) also note that AI, in conjunction with blockchain technology, can provide structure to decision-making in advanced healthcare systems for patient monitoring and diagnosis. Furthermore, Kuznetsov et al. (2024) emphasize that artificial intelligence combined with blockchain features does not merely secure data storage, but also applies logical structures to data han- dling. Only in environments such as healthcare do we see these models increasingly asserting their dependability.

E. Blockchain for Secure Data Sharing and Interoperability

However, since today's diverse independent systems are all technical islands, it is impossible to achieve this globally unified standard. But blockchain has the potential to alter this. It offers an open and safe framework for cross-platform data sharing across various healthcare

systems. According to Alghamedy et al. (2024), p. 113, blockchain technology allows various medical systems to collaborate and securely exchange data. Although all patient information is kept confidential, it is publicly disseminated among different healthcare organi- sations in a way that words alone might not adequately de- scribe.This is due to the fact that couplers, such as blockchain, exchange data in a global equilibrium. Additionally, they present various viewpoints and research questions that were not previously accessible to this extent. Thanks to its potential ability to serve as a general equilibrium solution for secure data exchange, blockchain not only provides interoperability between different systems so they can cooperate with each other, but also does so in a simple and effortless manner. In this way, medical professionals are able to read information without compromising patient privacy. Thus, quality and co- ordination are greatly enhanced.

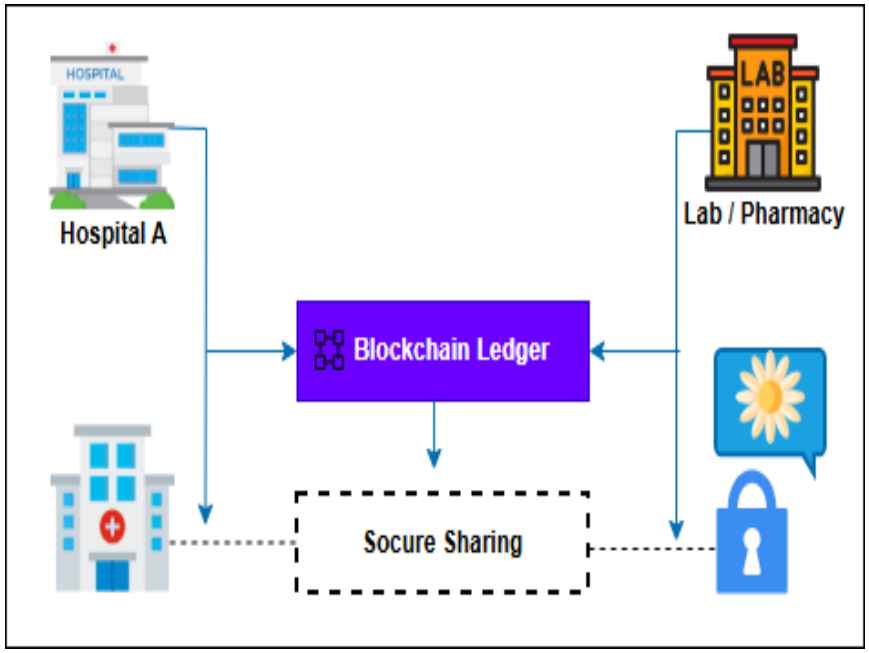

Fig. 3. Blockchain for Secure Data Sharing and Interoperability

In this model, healthcare organizations like hospitals, labs, and pharmacies can exchange information using a blockchain ledger system. Blockchain technology ensures the safe trans- mission of data through encryption and access control. The information about patients can be both viewed or edited by the Users who have signed up. Such a scheme is naturally conducive to maintaining interoperability between healthcare systems with adequate patient data privacy and confidentiality inside the blockchain.

F. The Use of Blockchain and AI to Enhance Security in IoT for Healthcare

In healthcare IoT network environment, blockchain (BC) along with artificial intelligence (AI) ensures efficient security management. Combined with AI, blockchain acts as a robust layer of security which can better secure medical data. Alamro et al. (2023) propose combining deep learning with Ant Lion Optimizer to improve intrusion detection in healthcare Internet of Medical Things (IoMT) networks. When we couple this with blockchain, the network enforces that only data from reputable and verified sources are allowed. This integration will greatly enhance the security and trustworthiness of health care apps. All IoMT readin... Vital health data is also written to the blockchain, designed so that it cannot be altered and only accessible by authorized users. Hence, this ensures the provenance of health data and that it is tamper-free. Kuznetsov et al. (2024)

emphasise again the necessity of combining blockchain to AI models to make sure that date used for AI training remain tamper-proof and fully traceable.

G. 6G Networks and Blockchain-IoT Integration

6G networks are envisaged to revolutionize the IoT space by offering ultra-reduced latency, extremely high data rate and largescale device association in a single network. The incor- poration of Blockchain and FL into 6G networks will form an ensure decentralized system ensuring large SCALES OF data (collected by IoT devices) to be managed. Alghamedy, et al. (2024) argue that, blockchain technology will play a leading role in securing data transmission in 6G networks; while FL ensures that machine learning models can be securely and collaboratively trained without compromising privacy of the data. These technologies combined in 6G networks offer real- time, secure communications now for a range of applications like smart cities, autonomous cars and industrial IoT.

H. The Future of Blockchain and Machine Learning Integra- tion in Healthcare

The combination of Blockchain and Machine learning in healthcare will be quite promising it is the Patients' Med- ical Health and Technology Future. According to Akrami et al. (2023), as the number of intelligent hardware devices in IoT ecosystems continues to increase the importance of Blockchain and Machine Learning in securing managing and analyzing healthcare data will grow Assuming the security and immutability of Blockchain plus using Machine Learning to forecast patient outcomes, find diseases and optimize treatment plans, the basic mode of operation for health systems is changed. In the 6G era described by Alghamedy et al. (2024), both Blockchain and Machine Learning are base technolo- gies. In this era of high-speed, low-latency networks when such systems may connect with other healthcare platforms or services yet ensure patient privacy is maintained over always-on connections across wide areas controlled potentially by different jurisdictions, these technologies will serve to harmonize data among various healthcare platforms.

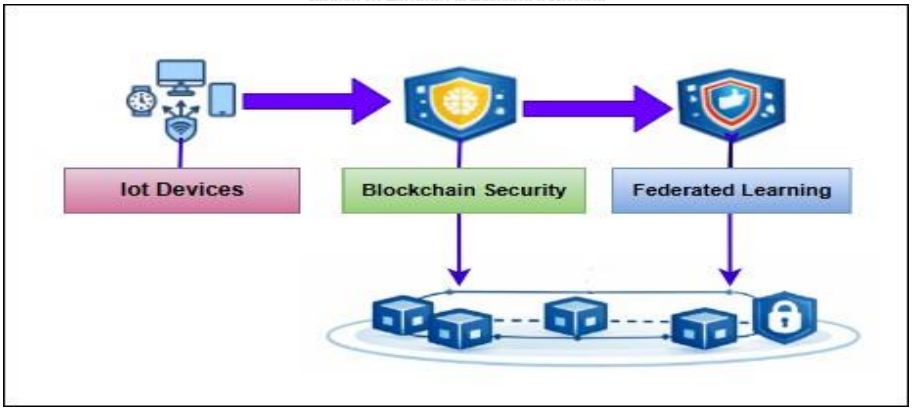

Fig. 4. Future of Blockchain and ML Integration in Healthcare

The IoMT products of the healthcare future will provide a large amount of information about patients. Blockchain technology will enable the stored information to be secure and distributed, and federated learning will help in training the models using Artificial Intelligence without affecting pa- tient information privacy. The collected information will be analyzed using AI. Hence, smart, secured, and patient-centric healthcare will be possible.

III. COMPARISON

Paper No.	Title	Dataset Used	Use Case	Advantages	Limitations
1	IoMT and Blockchain Synergy: A Novel Approach to Health Data Validation and Storage	Medical IoT data	Health data management	Secure data sharing, enhanced pri- vacy, interoperability	Limited generalizability to other in- dustries
2	Unlocking a Promising Future: Integrating Blockchain Technology and FL-IoT in the Journey to 6G	IoT device data	6G, IoT, federated learning	Future-ready for 6G, high scalabil- ity	Limited focus on practical imple- mentation
3	Unleashing the Potential of Blockchain and Machine Learning: Insights and Emerging Trends from Bibliometric Anal- ysis	Not applicable	Research analysis	Provides comprehensive insights on blockchain and ML integration	Focused on theoretical insights rather than practical use cases
4	Modeling of Blockchain Assisted Intru- sion Detection on IoT Healthcare System Using Ant Lion Optimizer with Hybrid Deep Learning	Benchmark intrusion datasets	IoT healthcare security	Enhanced intrusion detection using AI and blockchain	Performance depends on data qual- ity
5	On the Integration of Artificial Intelligence and Blockchain Technology: A Perspec- tive about Security	Various AI and blockchain use cases	AI and blockchain integra- tion	In-depth analysis of security con- cerns	Limited focus on healthcare imple- mentation
6	Unleashing the Potential of Blockchain and Machine Learning: Insights and Emerging Trends from Bibliometric Anal- ysis	Not applicable	Bibliometric analysis	Identifies trends in blockchain and ML research	Limited actionable recommenda- tions
7	Modeling of Blockchain Assisted Intru- sion Detection on IoT Healthcare System Using Ant	Healthcare IoT data	Intrusion detection in IoT healthcare	High detection accuracy and blockchain-based security	High computational resource re- quirements

	Lion Optimizer with Hybrid Deep Learning				
8	IoMT and Blockchain Synergy: A Novel Approach to Health Data Validation and Storage	Healthcare IoT data	Data validation and storage	Secure health data management	High implementation cost
9	Unlocking a Promising Future: Integrating Blockchain Technology and FL-IoT in the Journey to 6G	IoT devices and 6G networks	IoT and 6G integration	Improved privacy and security	Lack of real-world case studies
10	Modeling of Blockchain Assisted Intru- sion Detection on IoT Healthcare System Using Ant Lion Optimizer with Hybrid Deep Learning	Healthcare IoT data	Intrusion detection	Blockchain-based security improve- ment	Limited scalability beyond health- care
11	IoMT and Blockchain Synergy: A Novel Approach to Health Data Validation and Storage	IoMT data	Healthcare data validation	Improved interoperability	Limited scalability in non- healthcare sectors
12	Unlocking a Promising Future: Integrating Blockchain Technology and FL-IoT in the Journey to 6G	6G, IoT, federated learning	Blockchain and FL integra- tion	Privacy-preserving IoT systems	High deployment complexity
13	Modeling of Blockchain Assisted Intru- sion Detection on IoT Healthcare System Using Ant Lion Optimizer with Hybrid Deep Learning	Healthcare IoT data	Intrusion detection	Enhanced healthcare IoT security	Model complexity
14	IoMT and Blockchain Synergy: A Novel Approach to Health Data Validation and Storage	IoMT data	Health data storage and vali- dation	Ensures data integrity	Limited application outside health- care

15	Unlocking a Promising Future: Integrating Blockchain Technology and FL-IoT in the Journey to 6G	IoT, federated learning, 6G	Secure IoT network integra- tion	Addresses scalability and security	Lack of real-world deployment
16	Modeling of Blockchain Assisted Intru- sion Detection on IoT Healthcare System Using Ant Lion Optimizer with Hybrid Deep Learning	IoT healthcare data	IoT intrusion detection	Optimized security for healthcare IoT	Limited applicability to other sec- tors

IV. Research Methodologies

The methodological approaches of the reviewed papers include a wide array of techniques that often focus on Blockchain technology, FL, ML, and integrating these into IoT ecosystems. Specifically, the various methodologies employed in these studies can be further elaborated on as follows:

A. Blockchain Technology

Most of the reviewed papers utilize blockchain as the back- bone for data security and transparency. It is utilized mainly for secure data storage and dissemination in an environment where privacy concerns are higher, such as in healthcare. Permissioned blockchains, such as Hyperledger Fabric, were used in many instances to control access so that only the authorized participants can access the network. Blockchain's role in creating immutable transaction records ensures data integrity and traces changes to data.

In this regard, for instance, Ali et al. (2025) and Akrami et al. (2023) developed Blockchain-based systems that enabled secure data transmission and verification, which was neces- sary to ensure that IoT nodes within healthcare settings can communicate in a trustless manner.

B. Federated Learning

A federated learning system, a type of decentralized ma- chine learning, was used as a solution for data privacy issues that exist within IoT and healthcare applications. In FL, model training could be done collaboratively without having to share data. This was done without data disclosure because each of the participants had to do individual model training. This implementation was also done with blockchain technology to ensure all model updates shared among all participating nodes were authenticated and could not affect malicious activities. According to Alghamedy et al. (2024), FL is combined with Blockchain technology in a bid to ensure integrity in data utilized in collaborative machine learning tasks with a focus on protecting data poisoning attacks while building confidence in model updates, as per Alghamedy et al. (2024).

C. Machine Learning

Different applications in healthcare areas include intrusion detection and predictive analysis using Machine Learning algorithms, especially Deep Learning algorithms. For instance, Alamro et al. (2023) designed a hybrid Deep Learning model that included the combination of CNN and LSTM models for intrusion detection in IoT systems in healthcare. These models were optimized by using such algorithms as ALO to improve their performances. ML is not used only to analyze IoT datasets but also to make predictions about decisions in real-time processes.

D. *Datasets*

There were several benchmarking databases available, which have been utilized. For example, Alamro et al. con- ducted a study in 2023 and made use of the public intrusion detection database to test their designed models, while other studies made use of real-time health databases related to IoT. The databases proved to be very instrumental in ensuring that the designed methodologies for testing Blockchain and AI capabilities are correct within the real-time health sector.

V. Findings and Discussion

It is observed that the combination of Blockchain Technol- ogy and Internet of Things (IoT) and Machine Learning is proving to be revolutionary, which comes in a field such as healthcare where privacy and managing data in real-time is of utmost significance. From the review of various research papers, it is revealed that the significance and difficulties involved with these technologies are of utmost importance with reference to data privacy in healthcare and machine learning.

A. *Blockchain-Enabled Security*

The analysed papers have made it clear that Blockchain technology is a viable option to solve the issue of data security within an IoT scenario. Blockchain technology uses an immutable, distributed ledger to ensure privacy of sensitive health information. Ali et al. (2025) and Akrami et al. (2023) explain how Blockchain technology can ensure privacy of information, allowing anyone who is concerned, including pa- tients and devices within an IoT scenario, to share information completely while ensuring security.

B. *Federated Learning for Privacy-Preserving Machine Learning*

In most of the papers, FL was widely used to enable privacy- preserving machine learning. Because it keeps data in the local devices and transmits only the model updates, it minimizes data privacy. Thus, integration between Blockchain technology along with FL can ensure that the update of models is secure and also verified against malicious modification. Thus, this can be quite useful in IoT for healthcare, where sensitivity regarding data is at a higher level.

C. *Hybrid Models for Intrusion Detection*

Hybrid deep learning models combining CNN with LSTM for intrusion detection in IoT healthcare systems were ana- lyzed. Alamro et al. demonstrated that the models are resilient and efficient in securing IoT healthcare environments from cy- berattacks. This ensures that with Blockchain, the immutability and security of data being processed are already guaranteed.

D. *Applications in Healthcare*

The integration of Blockchain technology and ML in health care IoT applications is demonstrated to enhance data valida- tion, patient monitoring, and decision-making processes. For instance, Ali et al. in 2025 conceptualized a model where data is validated in real-time by Blockchain technology, ensuring data validity during AI-driven decision-making. Moreover, Alghamedy et al. in 2024 elaborated on how the integration of Blockchain and ML in health care IoT has resulted in remote patient monitoring, management of chronic patients, and resource distribution in health care.

E. *Practical Insights*

The research works offer real-world insights on how these technologies can be adopted. The challenge that repeats in these research works is the complexity of calculations in the hybrid models adopted in intrusion detection and real-time processing. The models, such as CNN and LSTM, consume considerable processing power, which may not be an issue with all IoT devices. The processing latency, however, may be an issue in real-time health applications.

VI. Challenges and Future Directions

In spite of the positive findings, challenges still persist in the integration between Blockchain, IoT and Machine Learning.

A. *Scalability*

Scalability in Blockchain technology is a significant hin- drance, and this is especially the case with the growing number of devices in the IoT environment. It is difficult to scale up Blockchain in the IoT environment based on the transaction processing capabilities of Blockchain in real-time applications. sharding, off chain transactions and other solutions like these may provide potential solutions but they need to be explored further for their security and practicality.

B. *Computational Complexity*

models that combine deep learning and hybridization are used for intrusion detection, predictive analytics, and other tasks. This requires significant computing resources. IoT de- vices that have limited processing power will struggle to support these models, even though powerful hardware can perform the tasks. Future research should be focused on light- weight models, and edge computation in order to distribute computations across the network and reduce the load on individual device.

C. *Data Privacy*

While Federated learning is a privacy-preserving solution, it still poses the risk of poisoning. This occurs when malicious updates are made to the model, which can degrade the perfor- mance. To prevent these attacks, future research should focus on advanced anomaly detector as well as AI based safeguards.

D. *Regulatory and Standardization Issues*

Lack of regulations and standards in the healthcare industry can hinder their adoption. Regulations need to address privacy issues and provide clear guidelines on the integration of these new technologies, especially in the contexts of cross-border sharing of data and compliance with regulations such as HIPAA and GDPR.

VII. Future Research Directions

A. *Integration with 6G Networks*

The soon-approaching era of 6G networks would make it imperative for the integration of Blockchain, Iot, and ML. This would help cater to the enormous number of devices that would be required for connectivity.

B. *AI-Driven Smart Healthcare Systems*

Research should focus on developing an AI-driven smart healthcare system to track patients' medical-related data auto- matically and provide analytics for predicting the outcome of the treatment based on the use of Blockchain technology for safeguarding patients' privacy.

C. *Blockchain-Enhanced IoT Security*

There is still research required in improving the consensus algorithm of Blockchain technology in handling large trans- action volume in massive-scale IoT networks, specifically in healthcare and industry IoT applications.

VIII. Conclusion

The collective use of Blockchain Technology, IoT, and Machine Learning holds immense potential that can cause a paradigm shift in the health care system because of the added benefits of secured data handling and decision-making. This is because Blockchain Technology provides a secured platform to deal and store health care information in a secure manner, and federated learning assists in implementing machine learning in health care while maintaining decentralization of the sensitive health care information. All these three pieces are required to be combined together to opt for a secured and efficient health care IoT. Despite this, there are still challenges such as scalability, complexity, and privacy concerns comprising the challenges to be overcome. The future research should therefore include development of a scalable Blockchain tech- nology, a lightweight AI technology, and a Federated Learning methodology for ensuring privacy. Additionally, the coming generation of communication networks referred to as the 6G network is expected to provide opportunities to combine the technologies mentioned above on a larger scale and will therefore be able to establish a smart healthcare environment.

References

A. S. M. Ali, S. Ali, K. Ziaullah, M.-I. Joo, and H.-C. Kim, "IoMT and Blockchain Synergy: A Novel Approach to Health Data Validation and Storage," IEEE Access, vol. 13, pp. 57753–57770, 2025, doi: 10.1109/ACCESS.2025.3555289.

F. H. Alghamedy, N. El-Haggar, A. Alsumayt, Z. Alfaweir, M. Alshammari, L. Amouri, S. S. Aljameel, and

S. Albassam, "Unlocking a Promising Future: Integrating Blockchain Technology and FL-IoT in the Journey to 6G," IEEE Access, vol. 12, pp. 115411–115433, 2024, doi: 10.1109/ACCESS.2024.3435968.

N. E. Akrami, M. Hanine, E. Soriano Flores, D. Gavilanes Aray, and I. Ashraf, "Unleashing the Potential of Blockchain and Machine Learning: Insights and Emerging Trends From Bibliometric Analysis," IEEE Access, vol. 11, pp. 78879–78894, 2023, doi: 10.1109/ACCESS.2023.3298371.

H. Alamro, R. Marzouk, N. Alruwais, N. Negm, S. S. Aljameel, M. Khalid, M. A. Hamza, and M. I. Alsaid, "Modeling of Blockchain Assisted Intrusion Detection on IoT Healthcare System Using Ant Lion Optimizer With Hybrid Deep Learning," IEEE Access, vol. 11, pp. 82199–82210, 2023, doi: 10.1109/ACCESS.2023.3299589.

S. Kuznetsov, P. Sernani, L. Romeo, E. Frontoni, and A. Mancini, "On the Integration of Artificial Intelligence and Blockchain Technology: A Perspective About Security," IEEE Access, vol. 12, pp. 3881–3898, 2024, doi: 10.1109/ACCESS.2024.3349019.

N. Akrami, M. Hanine, E. Soriano Flores, D. Gavilanes Aray, and I. Ashraf, "Unleashing the Potential of Blockchain and Machine Learning: Insights and Emerging Trends From Bibliometric Analysis," IEEE Access, vol. 11, pp. 78879–78894, 2023, doi: 10.1109/ACCESS.2023.3298371.

H. Alamro, R. Marzouk, N. Alruwais, N. Negm, S. S. Aljameel, M. Khalid, M. A. Hamza, and M. I. Alsaid, "Modeling of Blockchain Assisted Intrusion Detection on IoT Healthcare System Using Ant Lion Optimizer With Hybrid Deep Learning," IEEE Access, vol. 11, pp. 82199–82210, 2023, doi: 10.1109/ACCESS.2023.3299589.

A. S. M. Ali, S. Ali, K. Ziaullah, M.-I. Joo, and H.-C. Kim, "IoMT and Blockchain Synergy: A Novel Approach to Health Data Validation and Storage," IEEE Access, vol. 13, pp. 57753–57770, 2025, doi: 10.1109/ACCESS.2025.3555289.

F. H. Alghamedy, N. El-Haggar, A. Alsumayt, Z. Alfaweir, M. Alshammari, L. Amouri, S. S. Aljameel, and

S. Albassam, "Unlocking a Promising Future: Integrating Blockchain Technology and FL-IoT in the Journey to 6G," IEEE Access, vol. 12, pp. 115411–115433, 2024, doi: 10.1109/ACCESS.2024.3435968.

M. Alamro, R. Marzouk, N. Alruwais, N. Negm, S.

S. Aljameel, M. Khalid, M. A. Hamza, and M. I. Alsaid, "Modeling of Blockchain Assisted Intrusion Detection on IoT Healthcare System Using Ant Lion Optimizer With Hybrid Deep Learning," IEEE Access, vol. 11, pp. 82199–82210, 2023, doi: 10.1109/ACCESS.2023.3299589.

A. S. M. Ali, S. Ali, K. Ziaullah, M.-I. Joo, and H.-C. Kim, "IoMT and Blockchain Synergy: A Novel Approach to Health Data Validation and Storage," IEEE Access, vol. 13, pp. 57753–57770, 2025, doi: 10.1109/ACCESS.2025.3555289.

F. H. Alghamedy, N. El-Haggar, A. Alsumayt, Z. Alfaweir, M. Alshammari, L. Amouri, S. S. Aljameel, and

S. Albassam, "Unlocking a Promising Future: Integrating Blockchain Technology and FL-IoT in the Journey to 6G," IEEE Access, vol. 12, pp. 115411–115433, 2024, doi: 10.1109/ACCESS.2024.3435968.

M. Alamro, R. Marzouk, N. Alruwais, N. Negm, S.

S. Aljameel, M. Khalid, M. A. Hamza, and M. I. Alsaid, "Modeling of Blockchain Assisted Intrusion Detection on IoT Healthcare System Using Ant Lion Optimizer With Hybrid Deep Learning," IEEE Access, vol. 11, pp. 82199–82210, 2023, doi: 10.1109/ACCESS.2023.3299589.

A. S. M. Ali, S. Ali, K. Ziaullah, M.-I. Joo, and H.-C. Kim, "IoMT and Blockchain Synergy: A Novel Approach to Health Data Validation and Storage," IEEE Access, vol. 13, pp. 57753–57770, 2025, doi: 10.1109/ACCESS.2025.3555289.

F. H. Alghamedy, N. El-Haggar, A. Alsumayt, Z. Alfaweir, M. Alshammari, L. Amouri, S. S. Aljameel, and

S. Albassam, "Unlocking a Promising Future: Integrating Blockchain Technology and FL-IoT in the Journey to 6G," IEEE Access, vol. 12, pp. 115411–115433, 2024, doi: 10.1109/ACCESS.2024.3435968.