International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Blockchain-Integrated Federated Learning for Secure Patient-Centric Care in Healthcare 5.0

Dr. Rahul Srova[1], Dr. Trinjana Sachdeva[2], Dr. Archana Shahi[3]

[1,2]Researcher, Department of Hospital and Healthcare Administration, Baba Farid University of Health Sciences
[3]Assistant Professor, Department of Hospital and Healthcare Administration, Baba Farid University of Health Sciences

ABSTRACT
Healthcare 5.0 shows an evolution in intelligent, integrated, and patient-centric health systems, which is based on the interconnected use of technologies such as Internet of Medical Things (IoMT), Artificial Intelligence (AI) and edge computing. But, with increasing dependence on these technologies, it also causes several concers, such as data privacy, security, and interoperability. The sharing of data at one centre for training can increase the risk of data breach, raising worries about data safety. Federated learning, on the other hand, allows training of machine learning models without sharing data in a decentralised manner. The patient privacy and data remain protected as sensitive data can remain on the device. Simultaneously, Blockchain improves this framework by providing a secure and transparent record of data transactions, providing accurate data tracking which further reduces the risk of data tampering. In this paper, we will evaluate the integration of Federated learning with blockchain technology in the framework of Internet of Medical Things (IoMT). We present a system design which guarantees secure data exchange, reliable model aggregation and traceability. Additionally, We will also discuss about challenges and ethical consideration in its implementation.

Keywords: Blockchain, Federated Learning, IoMT, Healthcare 5.0, Data Privacy

INTRODUCTION

Over the years, healthcare industry faced a transformative journey. It has transformed from conventional clinic model to an interconnected smart healthcare model. Healthcare 1.0 represented the traditional model, in which care was given primarily with physical interaction between doctor and patients, as shown by ***Kaur et al. (2021)***. With Healthcare 2.0 model, electronic health records, diagnostic imaging, life support techniques were introduced. Further, the Healthcare 3.0 brought the philosophy of patient-centered care, which delivers care around the patient experiences. With the rise in telemedicine, patients can access the care remotely. However, it was not able to process large and real-time data, which limited its effectiveness and implications. This difference was solved with Healthcare 4.0 model. With the advancements like smart wearable devices, sensors, and Internet of things (IoT), it was able to analyze large and real time data, allowing us to perform continuous monitoring and enhancing our decision making, as explained by ***Aggarwal et al. (2021).***

The growing demand of a smart, intelligent and automated healthcare shows us the need of Healthcare 5.0 model. Healthcare 5.0 is a critical change in the modern medicine which brings technology and

patient-centered care together. At the centre of this change, there is an interconnected system of intelligent solutions powered by Artificial intelligence (AI), the Internet of Medical Things (IoMT). In contrast to the previous healthcare versions, Healthcare 5.0 is more aligned with future (anticipatory) care, where proactive personalizes interventions replace reactive ones, ultimately aimed at empowering patients, improving clinician decision-making, and increasing system efficiency, as mentioned by ***Aceto et al. (2020).***

With the rise of IoMT devices including smartwatches and biosensors, as well as AI-powered diagnostic tools, we now have a constant flow of real-time data that is invaluable for personalized care. But these devices, too, leave patients at risk of a digital vulnerability. As the more data passes between 2 points, the risk of hacking, unauthorised access, and misuse of the data increases, as shown by ***Xu et al. (2022).*** Conventional centralized health data systems are known to be inadequate for addressing such challenges, as they typically do not scale, are not resilient, and do not have trust models that can be used for the purpose of securely governing sensitive data, as mentioned by ***Khan et al. (2023).***

Justicia et al. (2021) suggested federated learning offers a possible solution by enabling us to train AI models at local decentralised centers without the need of sharing the patient's personal data to a common centralised point**.** As highlighted by ***Li et al. (2020),*** the hospitals can train their AI models, while keeping their data on their own server. They only need to share model updates, not the actual data with each other, by which the risk of data hacking is reduced, as shown by ***Li et al. (2020)***. But, along with these great uses, it still has challenges such as preventing unauthorised access to the data. At this stage, blockchain technology can offer a great solution by making our data access more trustworthy and transparent. After first being introduced by ***Nakamoto (2008***) for cryptocurrency, it has also been expanded to privacy protection, finance, cloud services, the Internet of Things (IoT). Combined with federated learning, the blockchain adds an extra layer of learning to the system, which makes a digital record of who accessed the data, when they accessed it, and what they did with it, as explained by ***Yang et al. (2022). Singh et al. (2020)*** showed that blockchain also provides features like smart contracts, promoting automation in this framework. It can automatically decide who can log in to this network to prevent unauthorised access.

There are great uses of this interconnected model in the healthcare industry. It can continuously monitor patients with diabetes, cardiovascular diseases, or chronic respiratory diseases by using wearable devices, as mentioned by ***Abdulmalek et al. (2022).*** Local federated learning models can help in identifying early warnings and suggesting personalized interventions. Thus, by integrating blockchain with federated learning (FL), sensitive data can be safely stored and used to learn without the need to send it to a central server. ***Asif et al. (2022)*** highlighted the possible implication of telesurgery, where doctors can perform distant surgeries with wireless fast communications while ensuring secure data without storing sensitive data in a centralized location. Additionally, it can also help in minimizing the frauds in health insurances. Fraudulent health insurance is a constant issue in every healthcare system globally, and it burns down the resources and causes a decline in trust. Blockchain-based federated learning (FL) is a promising approach since it allows a decentralized analysis of claims data in a way that does not affect the privacy of the policyholders. Using this method one can detect suspicious patterns and anomalies across various sources and all that without the sensitive information actually going anywhere. The system is also improved by smart contracts that automate the fraud detection protocols eliminating the need to waste time and make an evaluation of claims more transparent and

smooth. All these technologies open the path toward a safer, smarter, and responsible insurance ecosystem, as explained by ***Kapadiya et al. (2022).***

The combination of blockchain and Federated Learning in Healthcare 5.0, in short, is nothing less than a reimaginations of digital health that posits how trust, privacy, and intelligence in a digital environment can coexist without compromising other aspects of digital health. It provides an infrastructure to secure, scalable, participatory systems of healthcare, which consider scientific rigor and human dignity. In this complex world of coverage, there is a main rule that evades our attention- the future of healthcare should become not only highly ethical but highly intelligent, should not only be highly connected but highly private.

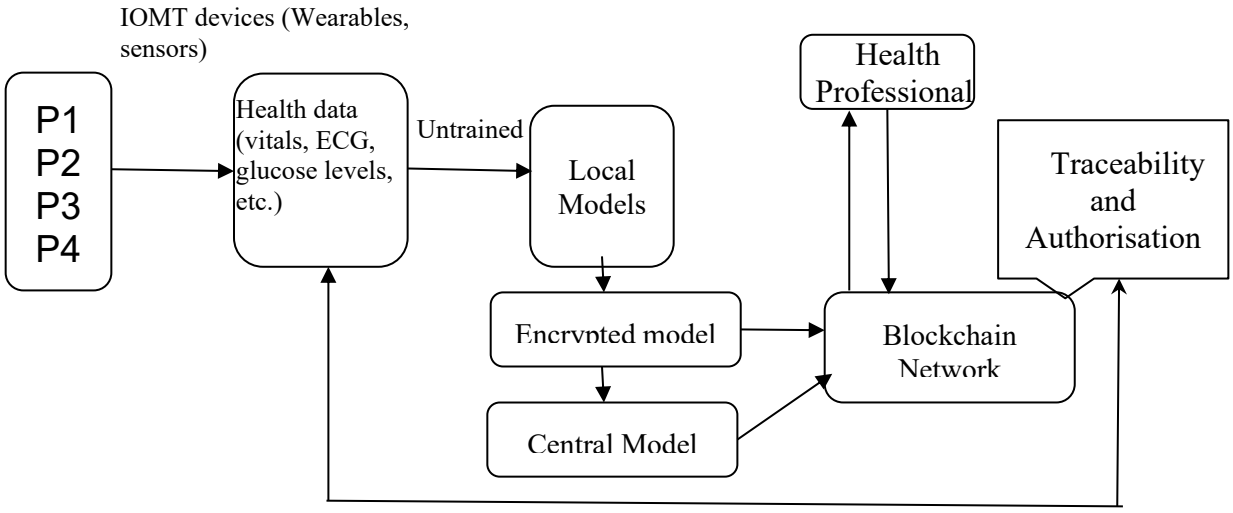

Figure 1. Simplified framework of blockchain with federated learning in Healthcare 5.0.
Source: Self-created, adapted from ***Khan et al. (2023).***

LITERATURE REVIEW

The traditional healthcare model has evolved from physical meetings of patients and doctors at clinics to the smart, interconnected, and automated healthcare system. ***Rehman et al. (2022)*** highlighted the difficulty of visiting doctor's clinics and hospitals for their treatment due to time management and risk of hospital-associated infections. The risk of acquiring infections at hospitals increases on visiting the hospitals, as shown by ***Graves et al. (2007).*** Now, people are shifting to telemedicine, where they can access the treatment and care at a distance with wireless communications. This system monitors patient data such as blood pressure, heart rate, blood saturation, temperature, glucose readings, etc, remotely which can be sent to physicians at distant places. All of this has become reality due to fast internet connections, Internet of Medical Devices (IMOT), and powerful computing levels. The integration of AI learning models into this model facilitates us to have early predictions based on health data and personalised interventions, resulting in patient-centric care.

However, sharing patient's health-related private data with other centers for learning models increases some concerns. The continuous sharing of data and storing it in a central location can increase issues related to privacy and security of the data, as shown by several studies such as ***Li et al. (2023), Awan et al. (2019), and Jaimes et al. (2023).*** Federated learning emerges as a possible solution to these concerns

by storing data at local computers and training models at decentralized areas and sharing only local model updates to the central area, not the personal patient data. Federated learning has gained popularity nowadays globally due to strict data privacy laws, as expressed by ***Yoo et al. (2022)***. As, the conventional learning requires large amount of training data to the centralised servers, the federated learning introduces a decentrailised learning model, allowing training of models at multiple devices locally. On the privacy scale, its advantage is that the possibility that research and development of AI models do not require the collection of sensitive client information is a major plus.

In his study, ***Srova (2025)*** has shown the possible role of AI models in reshaping the public health. He stated that by integrating public health and Healthcare 5.0, we can have predictive analysis reshaping disease prevention, personalised care, resource optimization, further highlighting the importance of federated learning. As stated by ***Srova and Shahi (2025)***, focusing on resource optimization and improving operation efficiency will also increase sustainability of healthcare services. It will enable us to analyze large amount of data from EHR (electronic health records), which will help us in disease surveillance and outbreak predictions. ***Shahi (2025)*** also highlighted the role of digital health tools such as machine learning, telemedicine, and wearables with biosensors in contributing to health promotion, disease prevention, and enhancing public health. In another study, ***Shahi and Mittal (2024)*** further discussed about the potential of federated learning in revolutionising existing medical therapeutic approaches, infrastructures, and the overall patient experiences. ***Shahi et al. (2024)*** further showed that combining robotic-operated surgery with AI analytics is a very big step towards highly accurate delivery of healthcare. Such systems can be advantageous when integrated into Federated learning systems as some intelligence can be shared within an institution without the risk of sensitive surgical information being shared.

The data collected from Electronic Health Records (EHR) is generally scattered at various institutions, making it difficult for us to use them effectively. Federated learning is a great solution to this issue by allowing these various institutions, including hospitals and clinics to train their models locally with these EHRs without the need of sharing it to central server, as highlighted by ***Joshi et al. (2022). Reddy et al. (2023)*** also stated that federated learning can help us in advancing mental and physical well being by its ability to process and learn from vast amount of data generated by healthcare industry with low concerns of data privacy and security.

Although having such great applications, there are also some challenges related to technical aspects and efficiency. ***Yang et al. (2019)*** have highlighted one of the main challenge of FL i.e. leaking of data while the training process of the models. These type of challenges need additional layer of safety, such as homomorphic encryption. Integration of blockchain and FL has capabilities to record a secure record, which cannot be changed later, further enhancing its transparency.

Esposito et al. (2021) noted that primary function of blockchain in healthcare was to improve accuracy and secure access to the data. But later, it also became relevant in the field of federated learning through its transparent and secure framework while training models at local centers. ***Houda et al. (2022)*** showed the ability of blockchain to secure decentralised model training with the data collected using IoMT devices and detect anomalies in the system without compromising patient's privacy. In their study, ***Tlemçani et al. (2025)*** worked on possible solutions for maintaining privacy in FL in healthcare. The differential privacy approach, the homomorphic encryption approach, and the blockchain-based trust approach were identified as there main approaches. Out of these, blockchain-enabled FL technologies was found to have most secure and useful approach in decentralised federated learning. Their study

showed that blockchain technology could improve security of federated learning, from the start of data collection for learning of the AI model to the last sharing updates of trained models.

The importance of integrating blockchain with Federated learning (FL) in healthcare systems was also studied by ***Limbepe et al. (2025)***. Their study highlighted the advantage of using federated learning along with blockchain technology in encrypted format for collecting data by using IoMT devices and training models at decentralised locations. When this framework used along with technologies like SMPC, it easily fulfils the security requirements of GDPR and HIPAA.

Data ownership and consent for using that data is an important worry in blockchain supported federated learning. The use of smart contracts by patients to control the permission of accessing the data was demonstrated by ***Christidis et al. (2016).*** Such approach also connects to the idea of ethical AI and contributes to patient-centered care by placing patients at the centre of care. In this model, the privacy of data is guaranteed by the use of smart contracts, so that privacy does not depend on manual verification.

Nguyen et al. (2021) shown that during the period of health crises such as COVID-19, federated learning with blockchain was highly effective for tracing contacts and symptoms. Their study showed decentralised learning models performed very well in COVID-19 pandemic, while securing privacy. It highlighted the potential of these models in public health emergencies.

Overall, the literature indicates that it is evidence of the scalable and feasible solution that blockchain-integrated federated learning can be suggested to the Healthcare 5.0. The systems solve major obstacles to the diffusion of AI in the clinical environment, such as privacy, trust, and transparency. Working on developments in cryptography and edge computing and distributed consensus, researchers and practitioners are constructing resilient frameworks in line with ethical, legal, and technical imperatives.

RESEARCH QUESTIONS

The research will focus on the following questions:

RQ1: What can be done to incorporate the federated learning using the blockchain mechanism to maintain the privacy and security of patient data in Healthcare 5.0?

RQ2: How well does blockchain-entrenched FL boost trust, transparency and traceability in decentralized patient monitoring systems?

RQ3: What is the compatibility between the regulations of global data protection projects like GDPR and HIPAA with the existing blockchain-FL architectures?

RESEARCH OBJECTIVES

The following objectives will be focused:

O1: Design and analyse a blockchain integrated federated learning framework with secure and privacy preserving process of patient data within Healthcare 5.0 settings.

O2: To assess how integration of blockchains and FL can enhance trust, transparency and traceability in the process of real-time patient monitoring.

O3: To evaluate the compliance of the current blockchain-FL healthcare models with the existing international data protection laws.

RESEARCH QUESTIONS, OBJECTIVES, AND HYPOTHESES

Research Questions	Objectives	Hypotheses
RQ1: What can be done to incorporate the federated learning using the blockchain mechanism to maintain the privacy and security of patient data in Healthcare 5.0?	O1: Design and analyse a blockchain integrated federated learning framework with secure and privacy preserving process of patient data within Healthcare 5.0 settings.	H0: No increase in privacy and security significantly. H1: Great enhancement in the privacy and security.
RQ3: How well does blockchain-entrenched FL boost trust, transparency and traceability in decentralized patient monitoring systems?	O2: To assess how integration of blockchains and FL can enhance trust, transparency and traceability in the process of real-time patient monitoring.	H0: No enhancement in trust, transparency, or traceability. H1: Significant enhancement in trust, transparency, or traceability.
RQ4: What is the compatibility between the regulations of global data protection projects like GDPR and HIPAA with the existing blockchain-FL architectures?	O3: To evaluate the compliance of the current blockchain-FL healthcare models with the existing international data protection laws.	H 0: Nothing more compliant than conventional systems. H1: GDPR and HIPAA compliance improved.

Table 1: Research Questions, Objectives, And Hypotheses

METHODOLOGY

This paper adopts the Systematic Literature Review (SLR) research methodology as a means of discussing how to combine federated learning (FL) and blockchain technology in developing secure, patient-centric care during the Healthcare 5.0 era. The SLR will enable the researcher to study a wide variety of secondary sources in the form of peer reviewed journal articles and proceedings to events such as conferences and give the research a grounded structure and evidence base.

The rationale behind the usage of SLR was based on the fact that it allows exploring the present academic environment comprehensively, openly, and without bias. The researcher retrieved raw data, available in recognized databases, namely IEEE Xplore, ScienceDirect, PubMed, and SpringerLink, to be sure that only high-quality relevant studies developed between 2000 and 2025 were used. The selection was conducted by using specific search terms i.e., blockchain AND federated learning AND healthcare, and privacy-preserving AI AND IoMT.

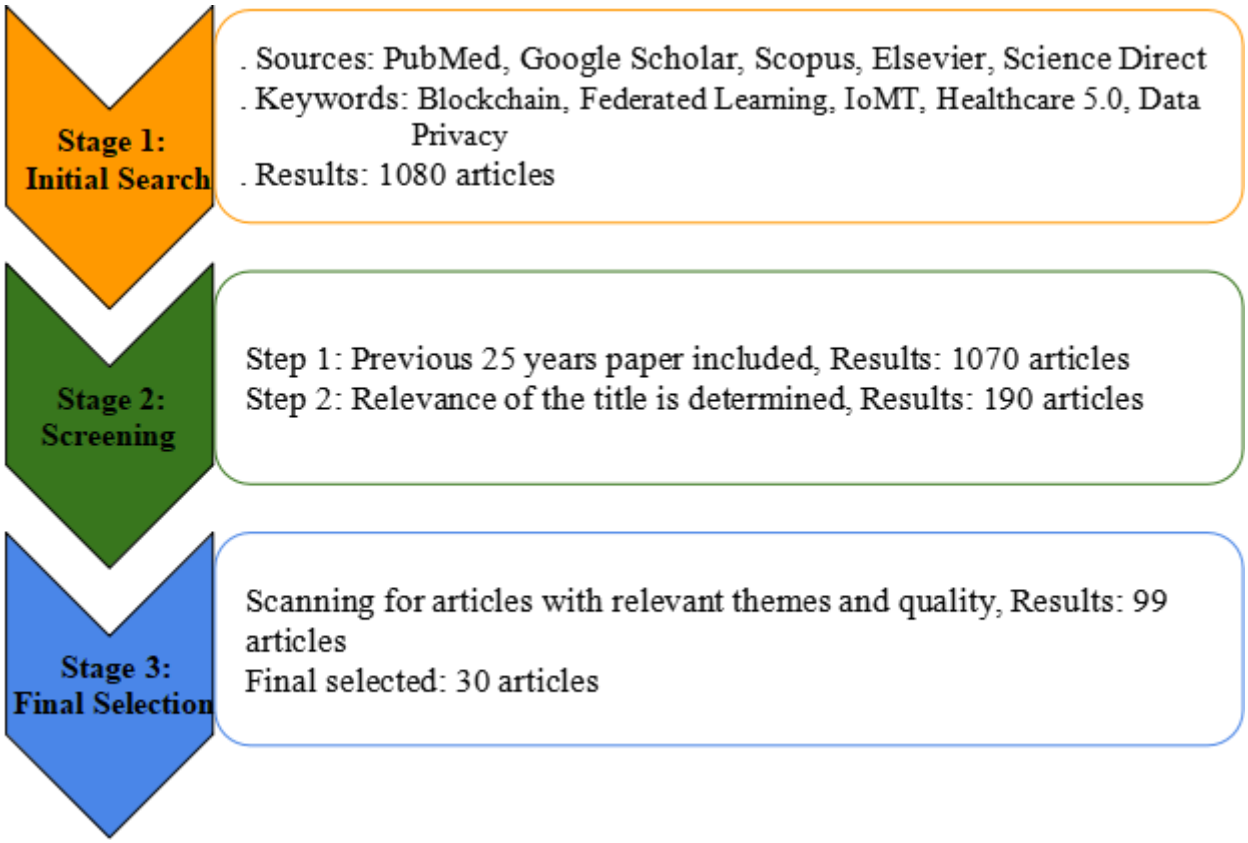

Figure 2: Flow chart of literature review

By means of this methodology, the researcher managed to trace the history of the development of decentralized learning in the field of healthcare, outline the major tendencies and issues, and fill in the research gap, using the previous works. The articles were filtered and evaluated by their relevancy, clarity of style, the method rigour, and their contribution to the field. Studies that approached the issues of privacy, trust, traceability, and regulatory compliance in blockchain-FL systems were only kept.

The SLR is helpful in making an informed decision as well as improving the academic credibility of the study. It is time-saving, reduces possible redundancy, and guarantees that new and meaningful work is done. In addition to that, this leads to transparency and replicability which makes the research process more authentic and scientifically sound.

The synthesis of knowledge found in various fields allows the SLR to become a strong foundation of the present study and a source of future actions targeted at the creation of ethical, scalable, and secure artificial intelligence systems in the healthcare sector.

DISCUSSION

Blockchain potential application in the field of federated learning provides innovative answer to some of the key issues that the healthcare sector is struggling with, as it evolves into the healthcare 5.0 environment. This paper emphasizes that the intersection of these technologies has a considerable potential to increase data security, patient privacy, and trust towards digital health all the way to improving the efficiency and intelligence of AI-based solutions.

The fact that this integration sustains data at the point of origin is a key strength of the integration. The federated learning technology allows training local models on devices like wearables, sensors, and

hospital systems, so that raw patient data never leaves the local machine or even goes to a central store. In addition to eliminating the chances of losing data, this strategy will allow increased patronage as the patients will feel in control of their personal data. Blockchain augments this by also recording model updates, access events and decision logic in an open and immutable ledger. This indisputable record also enhances the accountability of the system as well as allows all stakeholders trace activity and check results.

The system is also enhanced through rules mapped by smart contracts made to overrule the rules. In the case of patient consent management, establishing access to data, and ensuring node involvement in the federated network, smart contracts introduce a flexible and trustable mechanism of control. This facilitates the evolution of different data privacy rules and preconditions easier adherence to them by institutions and creates greater transparency of the whole system.

Other than privacy and compliance, architectures of blockchain based federated learning may enhance security of systems as well. They enable the anomaly detection online where the changes to the model are verified, and the detection of anomaly occurs in the case of adversarial or inconsistent behaviours. This is specifically applicable in medical field where there is no second chance to decisions and the system level failure can be dangerous. An extra layer of security implies that healthcare organizations fall into a safer path to use AI with much more confidence.

Nevertheless, numerous challenges have to be cleared in order to permit the mass adoption. Computational and blockchain innovation has the capability of causing a burden on systems, and more so the low-power systems. Moreover, it has a challenging issue of inter-organisational as well as inter-platform interoperability." And of course, the overhead of practical application also depends on human power, infrastructure and institutional support of ethical and innovation activities with data.

However, besides these challenges, it has huge potential for applications in the healthcare sector. It provides directions to healthcare institutions to work in collaboration without violating the privacy of the patients. It opens a path for us regarding safer use of AI in healthcare and achieving more patient-centered outputs.

APPLICATIONS AND PRACTICAL IMPLICATIONS

There are significant applications and practical implications of federated learning and blockchain in healthcare.

1. Nowadays, AI is the leading technology in the world. The AI with federated learning can increase accuracy and early diagnosis. It can be used in better treatment plans and patient-centric care.
2. Federated learning with IOMT devices enables continuous vitals and other health parameters monitoring of patient, which also aids in early and accurate diagnosis.
3. The decentalised training of models secure the privacy and integrity of the health data. When integrated with blockchain, the security of data further increases as it prevents unauthorised access to the data. The smart contacts powers patient to control who can access their data, further helping in patient-centeric care.

CHALLENGES AND FUTURE DIRECTIONS

This paper discusses several challenges in applying Federated Learning and Artificial Intelligence to healthcare, and realizing their full potential in improving patient care and health outcomes. Challenges to

data quality, data privacy and the problem of dealing with heterogeneous, decentralized datasets continue to require attention.

Going forward, it is anticipated that future work will involve the creation of stronger tactics and generalised approaches that are capable of effectively tackling these difficulties. Progress in these areas will be necessary to enable the full power of FL and AI in Healthcare 5.0—enabling systems that are intelligent and secure, as well as equitable and transformative, in the delivery of patient-centered care.

CONCLUSION

The paper focused on the intersection of blockchain and federated learning as a design-forward-thinking solution customized to fulfilling complex and changing needs of the Healthcare 5.0. Coupling the decentralization of computational potential that FL offers with the very features of blockchain of transparency, traceability, and immutability, the research is able to present a conceptual model which prioritizes the patient privacy, the integrity of the data, and adherence to the privacy requirements around the world.

The lessons learned through this discussion show that federated learning reduces the usage of central storage of data, which reduces the chances of data leakage and strengthens privacy between a patient and a healthcare provider. By combining it with blockchain, such distributed model becomes even more powerful, as the recorded information can be audited, access to the information is permitted through smart contracts, and compliance is designed into the framework, ensuring a secure and trusted infrastructure to be used by healthcare stakeholders.

The study confirms through systematic review of all existing sources that this approach addresses some of the most burning issues of digital health: their susceptibility to hacking, ill-readable management of data, and variable regulation compliance. Moreover, the strategy suggested can serve as a strategic baseline of possible implementations and improvement in the future.

Although there are some technical hurdles, such as an expanded computational load, the challenge of latency, and the interconnections of systems, emerging developments on the border between edge computing, lightweight blockchain architecture, and privacy-preserving technologies are continually coping with these obstacles. Therefore, the viability of blockchain-enhanced federated learning systems to be applied in the healthcare sector does not only seem plausible but become more critical by the day.

Altogether, the study contributes to the rising debate about safe, ethical, and patient-oriented digital health environments. It supports the necessity of joint, flexible and smart technological systems which will have the capacity to sustain city-resilient healthcare systems in a progressively connected and data-intensive planet.

Construct	Author(s)	Definition
Federated Learning (FL)	***Justicia et al. (2021)***	One that is based on distributed machine learning, which involves training of models in many devices without any raw data storage in a central hub.
Blockchain	***Esposito et al. (2021)***	A distributed ledger technology-based transaction recording on a peer to peer network that is

		verifiable and immutable.
Smart Contracts	***Christidis et al. (2016).***	Computer code installed in a blockchain that actively ensures rules and agreements without any human input.
IoMT (Internet of Medical Things)	***Aceto et al. (2020)***	A network of interrelated medical equipment which captures and shares health information in real time.
Data Privacy	***Xu et al. (2022)***	It is the act of defending the information concerning the personal health of individuals so that it is not accessed or revealed by other parties.
Trust and Traceability	***Khan et al. (2023).***	A capability to confirm the source and provenance of data or decision in a system, and improve credibility and reliability.
Compliance (GDPR/HIPAA)	***Limbepe et al. (2025)***	The compliance of data processing practices and systems to international regulations meant to control healthcare data protection such as GDPR and HIPAA.

Table 2: Constructs, Authors, And Definitions

REFERENCES

1. Kaur, J., Verma, R., Alharbe, N. R., Agrawal, A., & Khan, R. A. (2021). Importance of fog computing in healthcare 4.0. Fog Computing for Healthcare 4.0 Environments: Technical, Societal, and Future Implications, 79-101.
2. Aggarwal, S., Kumar, N., Alhussein, M., & Muhammad, G. (2021). Blockchain-based UAV path planning for healthcare 4.0: Current challenges and the way ahead. IEEE Network, 35(1), 20-29.
3. Aceto, G., Persico, V., & Pescapé, A. (2020). Industry 4.0 and Health: Internet of Things, Big Data, and Artificial Intelligence. *Journal of Industrial Information Integration*, 18, 100129. https://doi.org/10.1016/j.jii.2020.100129
4. Xu, R., & Ren, Q. (2022). Cryptoanalysis on a cloud-centric Internet-of-Medical-Things-enabled smart healthcare system. IEEE Access, 10, 23618-23624.
5. Khan, M. F., & Abaoud, M. (2023). Blockchain-Integrated Security for real-time patient monitoring in the Internet of Medical Things using Federated Learning. *IEEE Access*, *11*, 117826-117850.
6. Blanco-Justicia, A., Domingo-Ferrer, J., Martínez, S., Sánchez, D., Flanagan, A., & Tan, K. E. (2021). Achieving security and privacy in federated learning systems: Survey, research challenges and future directions. Engineering Applications of Artificial Intelligence, 106, 104468.

7. Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated learning: Challenges, methods, and future directions. *IEEE signal processing magazine*, *37*(3), 50-60.
8. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Satoshi Nakamoto.
9. Yang, Z., Shi, Y., Zhou, Y., Wang, Z., & Yang, K. (2022). Trustworthy federated learning via blockchain. *IEEE Internet of Things Journal*, *10*(1), 92-109.
10. Singh, A., Parizi, R. M., Zhang, Q., Choo, K. K. R., & Dehghantanha, A. (2020). Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities. Computers & Security, 88, 101654.
11. S. Abdulmalek, A. Nasir, W. A. Jabbar, M. A. M. Almuhaya, A. K. Bairagi, M. A.-M. Khan, and S. Kee, ‘‘IoT-based healthcare-monitoring system towards improving quality of life: A review,’’ Healthcare, vol. 10, no. 10, p. 1993, Oct. 2022
12. Al Asif, M. R., Hasan, K. F., Islam, M. Z., & Khondoker, R. (2021, December). STRIDE-based cyber security threat modeling for IoT-enabled precision agriculture systems. In 2021 3rd International Conference on Sustainable Technologies for Industry 4.0 (STI) (pp. 1-6). IEEE.
13. Chaudjary, S., Kakkar, R., Gupta, R., Tanwar, S., Agrawal, S., & Sharma, R. (2022). Blockchain and federated learning-based security solutions for telesurgery system: a comprehensive review. Turkish Journal of Electrical Engineering and Computer Sciences, 30(7), 2446-2488.
14. Kapadiya, K., Patel, U., Gupta, R., Alshehri, M. D., Tanwar, S., Sharma, G., & Bokoro, P. N. (2022). Blockchain and AI-empowered healthcare insurance fraud detection: an analysis, architecture, and future prospects. IEEE Access, 10, 79606-79627.
15. Rehman, A., Abbas, S., Khan, M. A., Ghazal, T. M., Adnan, K. M., & Mosavi, A. (2022). A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique. Com-puters in Biology and Medicine, 150, 106019. doi:10.1016/j.compbiomed.2022.106019 PMID:36162198
16. Graves, N., Weinhold, D., Tong, E., Birrell, F., Doidge, S., Ramritu, P., ... & Whitby, M. (2007). Effect of healthcare-acquired infection on length of hospital stay and cost. *Infection Control & Hospital Epidemiology*, *28*(3), 280-292.
17. Li, C., Dong, M., Xin, X., Li, J., Chen, X. B., & Ota, K. (2023). Efficient privacy preserving in IoMT with blockchain and lightweight secret sharing. IEEE Internet of Things Journal, 10(24), 22051-22064.
18. Awan, K. A., Din, I. U., Almogren, A., Guizani, M., Altameem, A., & Jadoon, S. U. (2019). Robusttrust–a pro-privacy robust distributed trust management mechanism for internet of things. IEEE Access, 7, 62095-62106.
19. Hernandez-Jaimes, M. L., Martinez-Cruz, A., Ramírez-Gutiérrez, K. A., & Feregrino-Uribe, C. (2023). Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud–Fog–Edge architectures. Internet of Things, 23, 100887.
20. Yoo, J. H., Jeong, H., Lee, J., & Chung, T. M. (2022). Open problems in medical federated Learning. International Journal of Web Information Systems, 18(2/3), 77–99. doi:10.1108/IJWIS-04-2022-0080
21. Srova, R. (2025). AI-POWERED PUBLIC HEALTH SYSTEMS: INNOVATIONS AND ETHICAL CONSIDERATIONS. Archives.
22. Srova, R., & Shahi, A. (2025). 24 Hospital Sustainability. *Sustainable Healthcare Systems in Africa: Technologies, Practices, and Management*, 466.

23. Shahi, A. (2025). DIGITAL HEALTH INTERVENTIONS: TRANSFORMING PUBLIC HEALTH SURVEILLANCE AND DISEASE PREVENTION. Archives.
24. Shahi, A., & Mittal, A. (2024). The Impact of Federated Learning on AI-Enhanced Healthcare Delivery. In Pioneering Smart Healthcare 5.0 with IoT, Federated Learning, and Cloud Security (pp. 57-66). IGI Global Scientific Publishing.
25. Shahi, A., Bajaj, G., GolharSathawane, R., Mendhe, D., & Dogra, A. (2024, April). Integrating Robot-Assisted Surgery and AI for Improved Healthcare Outcomes. In *2024 Ninth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)* (pp. 1-5). IEEE.
26. Joshi, M., Pal, A., & Sankarasubbu, M. (2022). Federated learning for healthcare domain-pipeline, applications and challenges. ACM Transactions on Computing for Healthcare, 3(4), 1-36.
27. Dasaradharami Reddy, K., & Gadekallu, T. R. (2023). A comprehensive survey on federated learning techniques for healthcare informatics. Computational Intelligence and Neuroscience, 2023(1), 8393990.
28. Abou El Houda, Z.; Hafid, A.S.; Khoukhi, L.; Brik, B. When collaborative federated learning meets blockchain to preserve privacy in healthcare. IEEE Trans. Netw. Sci. Eng. 2022, 10, 2455–2465.
29. K. Christidis, M. Devetsikiotis, Blockchains and smart contracts for the internet of things, Ieee Access 4 (2016) 2292–2303.
30. Nguyen, D. C., Ding, M., Pathirana, P. N., & Seneviratne, A. (2021). Blockchain and AI-based solutions to combat coronavirus (COVID-19)-like epidemics: A survey. *Ieee Access*, *9*, 95730-95753.