A Comprehensive Review of Blockchain and Federated Learning Integration for Secure Healthcare Systems

Hajer KHRIJI[1], Salim EL KHEDIRI[2], Salah ZIDI[3], Najoua BENNAJI[4]

1. National Engineering School of Gabes, ENIG, University of Gabes, Tunisia.
2. Department of Information Technology College of Computer Qassim University.
3. Higher Institute of Industrial System of Gabes, Tunis.
4. Higher Institute of Computer Science of Gabes, Tunis.

Email 1 : hajer.khriji@enig.rnu.tn
Email 2: salim.kdhiri@fsgf.ugaf.tn
Email 3: salah.zidi@univgb.tn
Email 4: najoua.bennaji@isimg.tn

Received	Accepted	Published
28/12/2025	19/01/2026	28/02/2026

DOI:https://doi.org/10.63939/JAAS.2026-Vol9.N28.51-63

Khriji, S., El Khediri, S., Zidi, S., & Bennaji, N. (2026). A comprehensive review of blockchain and federated learning integration for secure healthcare systems. *The Journal of Afro-Asian Studies*, 9(28), 51–63.

Abstract

The swift advancement and growth of Internet of Things (IoT)-based technologies have strengthened the way we live and our quality of life. Health is the most sensitive area of application of IoT given its relationship with human well-being. The use of IoT in healthcare is called the Internet of Medical Things (IoMT). It has become a booming trend aimed at improving the health and well-being of billions of people by providing seamless medical facilities and improving services provided by doctors, nurses, pharmaceutical companies and other governmental and related non-governmental organizations. The amount of data generated by the human body every day is two terabytes. We can now collect most of it by the advancement of these technologies including information on heart rate, sleep patterns, blood sugar, stress levels and even brain activity. That is why the security of this data, especially in real time, becomes a major concern. This article aims to explore the role of integration of Blockchain technology with federated learning in strengthening data security and ensuring privacy in healthcare sector. We aim to present a concise yet comprehensive overview of the Blockchain integration with federated learning in securing health data and ensuring privacy in the healthcare sector.

Keywords: *Healthcare, IoMT, Blockchain, Federated learning, Data security*.

1.Introduction

Traditionally, the main objective of healthcare focused on treating patients with medical interventions, leading to a lack of attention related to data privacy and safety (Patel et al., 2024, pp.18-46). In modern times, the healthcare sector has become pivotal for the holistic progress of countries across the globe. Due to increasing deployment of IoMT, a large amount of data is being generated. Data privacy, secure storage, the exchange of sensitive health information, and controlled access have emerged as the key concerns within today's healthcare system.

Artificial intelligence (AI) has accelerated the evolution of healthcare, primarily driven by the swift advancements in AI, cloud computing, machine learning, and blockchain technologies (El Khediri, 2025) (Wang et al., 2020, pp. 869-904). Machine learning (ML) and deep learning (DL) algorithms play a crucial role in revealing hidden patterns in healthcare data. Traditionally, data employed for training ML/DL algorithms was maintained in central storage facilities, which may result in several challenges, such as security issues, single points of failure, and heightened latency (Alpaydin, 2020).

With the aim of ensuring the security of patients' private data, several technologies have emerged, including IoMT, AI, blockchain, and federated learning (Casola et al., 2016, pp10-14). Since 2018, a significant surge has been witnessed in the adoption of blockchain technology in the healthcare sector (Hiwale et al., 2021, pp.190-213). Blockchain has gained widespread adoption because of its strong security features, such as immutability and cryptography, including the new concept of lightweight blockchain (Mershad & Cheikhrouhou, 2023, p100984). As a distributed, immutable, and append-only data structure, blockchain offers effective solutions to challenges faced by remote healthcare applications, improving transparency, security, trustworthiness, and authenticity of health data (Brogan et al., 2018, pp.257-266).

Recent literature has extensively examined blockchain applications in healthcare. Comprehensive research has evaluated the effectiveness of blockchain technology in healthcare (Agbo et al., 2019), addressed privacy challenges and preservation mechanisms (Bernabe et al., 2019, pp. 164908-164940), and introduced use cases while assessing unresolved concerns (Casino et al., 2019, pp.55-81).

Federated Learning (FL), an emerging technology, shows significant potential for enhancing healthcare data analytics while addressing concerns related to sharing sensitive information. Several studies have examined the recent advancements and challenges associated with federated learning in healthcare informatics, including future directions for this promising field (Xu et al., 2021, pp.1-19). FL enables entities to develop collaborative global models without sharing raw data with external parties (McMahan et al., 2017). A comprehensive categorization based on data distribution and privacy mechanisms (Bagdasaryan et al., 2020), and classification of security threats with strategies to improve privacy (Mugunthan et al., 2020).

Together, federated learning and blockchain technologies hold great promise for secure health data analysis and administration, offering complementary approaches to protecting patient privacy while enabling collaborative research and improved healthcare delivery. **Figure 1** illustrates advantages of combining blockchain with federated learning across various use cases. This paper is structured as follows: Following the introduction, Section II provides a comprehensive literature review; Section III explains how federated learning preserves privacy in healthcare; Section IV reviews how with its decentralized architecture, the blockchain helps to create a transparent healthcare workflow; Section V assures on the exploitation of these two technologies to guarantee enormous benefits in the healthcare sector; Section VI presents the discussion of this work; Finally,

in section VII, we present the conclusion.

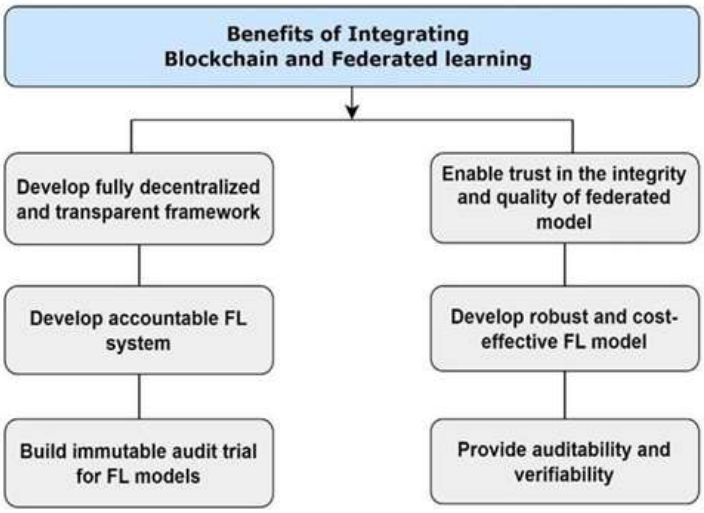

Fig. 1. Advantages of combining blockchain and federated learning for various applications

2.Literature review

Recent literature has extensively explored the application of federated learning and blockchain technologies in healthcare and IoT environments. Hao et al. provided a comprehensive overview of security benefits offered by federated learning in the health sector, emphasizing how this approach ensures private data remains protected (Li et al., 2023, pp. 8076-8094). Their analysis of potential attacks in medical environments highlighted the advantages of combining federated learning with blockchain to enhance security, particularly as healthcare data volumes continue to grow.

Several researchers have investigated the integration of blockchain with IoT systems. Dai et al. introduced the concept of Blockchain of Things (BCoT) (Ali, Salek, et al., 2018, pp. 1676-1717), outlining its core principles and examining challenges in merging blockchain with IoT infrastructures. Similarly, Ali et al. analyzed how blockchain addresses decentralization and security requirements in IoT networks, while proposing future research directions (Al Asqah & Moulahi, 2023, p.203).

Muneerah Al Asqah et al. provided an extensive review of how federated learning and blockchain can work together to improve security and privacy in IoT ecosystems (Pandl et al., 2020, pp. 57075-57095). Their work categorized existing solutions based on privacy preservation mechanisms, offering valuable insights into the integration of these technologies in distributed systems.

Despite these valuable contributions, few studies have conducted systematic literature reviews specifically examining the convergence of blockchain and federated learning for healthcare applications. Some notable exceptions include research by Dasaklis et al., who investigated the potential applications of combining intelligent systems with blockchain across various industries (Singh et al., 2020, p.102364), and studies by Singh et al., which explored how these emerging technologies can facilitate secure storage and sharing of patient data while improving overall care quality (Rieke et al., 2020, p.119).

- To perform an in-depth survey of existing literature on blockchain and federated learning aimed at advancing dependable healthcare applications.
- To examine and evaluate prior studies addressing the intersection of blockchain and federated learning approaches for ensuring privacy within healthcare systems.

- To highlight the benefits of combining blockchain with federated learning in safeguarding the security of patients' data.

Table 1: outlines various existing surveys in the literature that address security using Blockchain and federated learning solutions for the Internet of Things (IoT).

Proposed Work	Year of publication	Blockchain	Federated learning	Dedicated to IoT	Contribution
Hao et al.	2023	×	✓	✓	This work contributes significantly to the unterstanding of security issues related to federated learning (FL) in healthcare contexts
Dai et al.	2019	✓	×	✓	This work highlights the convergence of blockchain and IoT. Authors refer to « Blockchain of Things (BCoT) »
Viriyasitavat and al.	2019	✓	×	✓	This work highlights how the combination between blockchain and IoT technology can lead to enhanced security, transparency and efficiency in various application
Ali and al	2018	✓	×	✓	This work proposes a conceptual framework for integrating blockchain with IoT systems, providing a structured approach for researchers and practitioners to follow when implementing blockchain solutions in IoT
Pohrmen and al.	2019	✓	×	✓	This work proposes a framework for integration of blockchain with IoT architecture to improve security. This framework outlines how blockchain can be effectively utilized alongside traditional security mechanisms to create a more secure IoT ecosystem.
Muneera Al Asqah and al	2023	✓	✓	✓	This work proposes a framework that integrates federated learning and blockchain technology specifically aimed at enhancing privacy protection in IoT environments.
Y.Qu and al	2022	✓	✓	×	This work provides a comprehensive overview and evaluation of existing research on blockchain enabled federated learning, by categorizing different approaches and highlighting their strengths.
D.C.Nguyen and al	2021	✓	✓	×	This work introduces the concept of FL chain, a new paradigm that combines federated learning and blockchain to create decentralized, secure and privacy-enhancing systems.
S.Vyas and al	2019	✓	✓	×	This work introduces the concept of FL chain, a new paradigm that combines federated learning and blockchain to create decentralized, secure and privacy-enhancing systems.
S.Singh and al	2020	✓	✓	✓	This work provides a comprehensive overview of the potential benefits and use cases of integrating blockchain, AI and IoT for developing smart cities.

3.Federated Learning for data privacy in healthcare

3.1.Federated Learning

Federated learning is a new training method that uses machine learning models, yet maintains the confidentiality of the data. The models are also trained at several computers in a decentralized fashion instead of transferring sensitive patient data. In this system, all devices will construct a local model based on their own data and only send the learned model parameters or updates to a central server. This process will guarantee protection of privacy and provide collaborative learning among distributed sources. The federated learning architecture depicted by **Figure 2** depicts a typical example.

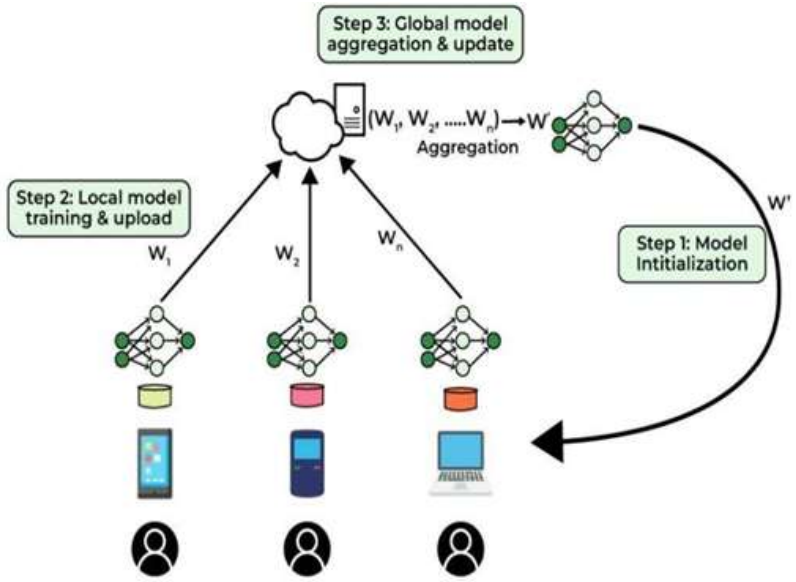

Fig. 2. Framework of federated learning

3.2. Preservation of Privacy in healthcare with federated learning:

Over the past two decades, machine learning (ML) models have developed into a powerful approach for attaining reliable and precise health data analysis. To fully utilize machine learning methods, a significant volume of health data is necessary to create efficient predictive models. Consequently, collaboration among multiple health organizations is essential for collecting and sharing medical information (Hussain et al., 2021, p.6985).

The COVID-19 pandemic underscored the critical importance of effectively sharing health data, resources, and expertise on a global scale (Donawa et al., 2019). However, the sensitive nature of medical information, coupled with strict privacy regulations such as HIPAA and GDPR, limits the ability of hospitals to exchange raw patient data with external entities. This situation creates a persistent tension between safeguarding confidentiality and enabling more accurate predictive data analysis (Dasaklis et al., 2018).

The concept of Federated Learning (FL) has great potential to solve this issue, as it allows training a global machine learning model without sharing raw data. Being a new paradigm, FL protects the privacy of data but helps develop collaborative models with the involvement of many contributors. Its main strength in comparison to traditional machine learning is the fact that it does not require centralization of sensitive data in repositories, thereby eliminating the centralization of this critical data. Training is instead done locally at the individual nodes, and only model updates are shared, thus obeying privacy laws like GDPR (Mothukuri et al., 2021, pp.619-640).

There are three main stages involved in the execution of federated learning:

1. The central server initially shares the global model parameters with all participating clients.
2. Each client trains a local model using its own dataset and the provided parameters, then transmits the updated model back to the server.
3. The server combines the updates from all clients to build a refined global model, which is redistributed to the clients for further iterations.

This iterative process continues until the model attains a designated level of accuracy (Christ et al., 2019).

The healthcare sector is one of the most influential fields where federated learning can be used. In that regard, FL allows hospitals to train a global model together, retaining the privacy of raw patient data. Rather than transmitting sensitive records, the institutions transfer locally trained model updates to a central server that combines them into a single predictive model. This will not only protect privacy, but also guarantee compliance to legal and ethical standards (Hewa et al., 2021, p.102857) (Ulhaq & Burmeister, 2020).

Several important applications of federated learning were proposed during the COVID-19 pandemic. E.g., the Stanford Institute of Human-Centered Artificial Intelligence developed a framework that would allow tracking people with coronavirus symptoms at home. Meanwhile, NVIDIA Clara released a healthcare platform based on federated learning that ensured data privacy of patients in medical organizations (Nakamoto, 2008). The representative scheme of federated learning in healthcare is presented in **Figure 3**.

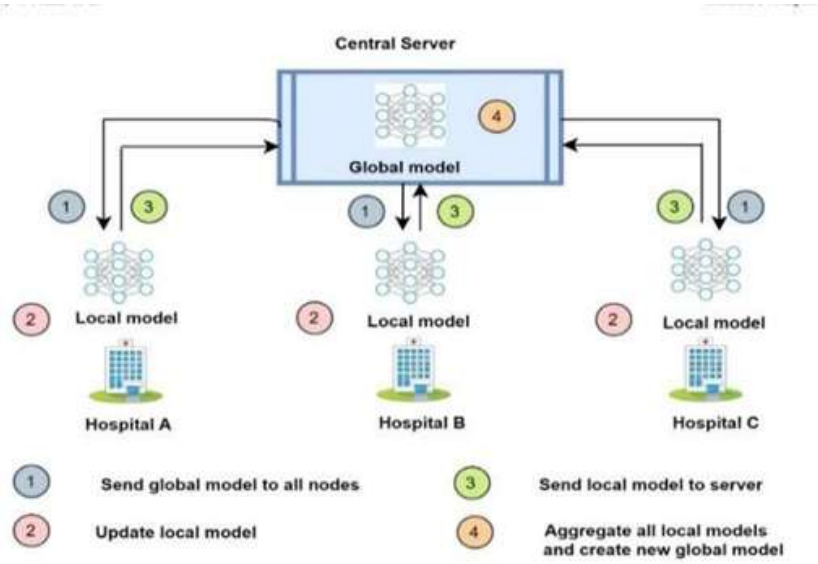

Fig.3. Structure of federated learning in medical contexts

Unlike traditional ML methods, FL inherently offers privacy protection. In federated learning scenarios, multiple hospitals collaborate to train models without centralizing their datasets. Hospitals exclusively transmitted their revised models to the coordinating servers. Consequently, the federated learning eliminates the need to aggregate extensive patient dat in any primary database. The federated learning decreased both costs and the time of training and while enhancing data security. **Table 2** outlines the benefits and challenges associated with federated learning.

Table 2. Advantages and obstacles of federated learning

Benefits	Obstacles
Enhance Scalability	Data heterogeneity
Enhance security and precision	Lack of universal solution
Protect privacy	Cost of time
Inexpensive training costs	Prospective privacy
Decrease the time of training	Expenses of communication

4.Blockchain-based healthcare solutions

4.1. Blockchain

It is a distributed, decentralized digital ledger that records transactions across various computers in a network. The blockchain consists of blocks, each containing multiple transactions. Each time a new transaction takes place, it is recorded and incorporated into the ledger of every participant. Blockchain uses cryptographic signatures called hashes to link blocks together, causing it to be very hard to modify or infiltrate the system. **Figure 4** explains how blockchain works.

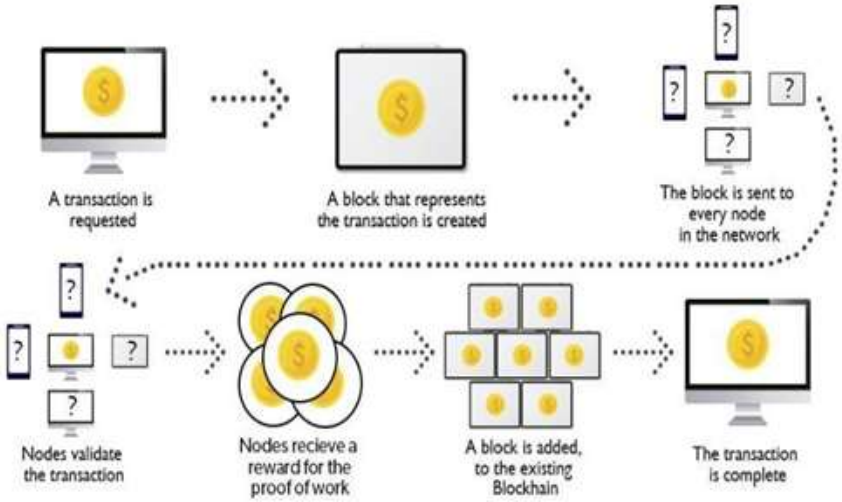

Fig.4. How blockchain works

4.2. Blockchain a solution in healthcare

The blockchain is a structure based on the distribution of data that is immutable and allows for append-only operations. Initially, the financial sector was the primary application of blockchain technology in the form of Bitcoin (Dasaklis et al., 2018). In recent times, thanks to its fundamental strengths, blockchain has proven to be highly adaptable across several fields beyond finance (Agbo et al., 2019). The healthcare sector holds immense potential for blockchain technology to drive a technological revolution. The decentralized and immutable characteristics of blockchain enable the creation of transparent healthcare workflows, allowing patients to monitor how their health data is shared and accessed within the system (Zheng et al., 2020, pp. 475-491). Furthermore, blockchain employs cryptographic algorithms to guarantee data security (Kuo et al., 2017, pp. 1211-1220). From a healthcare standpoint, the notable benefits of blockchain such as data provenance, accountability, availability, and robustness significantly enhance effective health record

management (Kang et al., 2018, pp S76-82). The technology facilitates secure, unchangeable, and expandable data exchange from diverse origins, including electronic health records (EHRs), clinical trials, genomic databases, and IoT data from numerous sensors (Ghosh et al., 2023, p38). Blockchain's focus in the health sector centers on creating secure systems for patient data management and secure transactions. Its tamper-proof characteristics, smart contracts, and data security solutions revolutionize healthcare operations, while in other sectors blockchain primarily serves for financial transfers, personal data security, and logistics (Yazdinejad et al., 2020, pp. 2146-2156). **Table 2** emphasizes the advantages and obstacles linked to blockchain technology. Several studies have examined blockchain's potential to transform healthcare information sharing. The following synthesis highlights an overview of pertinent research on blockchain-enabled healthcare solutions. Research by Tripathi, Ahad, & Paiva (2020) highlights how blockchain's decentralized nature eliminates single failure points and third-party dependencies, enabling efficient health data sharing. Similarly, Tomaz et al., (2020) demonstrates that blockchain's immutable, time-stamped transaction records foster trust and transparency in health information exchange. Smart contracts have been shown to facilitate patient-centered data access while enhancing security and promoting reliable information exchange among providers (Motohashi et al., 2019, p. e13385). According to Akkaoui et al., (2020, pp.113467-113486), blockchain's distributed, immutable, and transparent characteristics ensure safe and efficient data exchange among healthcare stakeholders and patients. Further research (Li et al., 2019, pp.2042-2053) reveals that smart contracts enable secure interactions between healthcare participants and clinical applications, addressing issues of permitted access and verification. When combined with smart contract logic, blockchain facilitates personalized and efficient electronic health record management, addressing security and interoperability challenges (Ndayizigamiye & Dube, 2019). Finally, Aich et al., (2022) emphasizes how blockchain ensures data provenance through traceability and immutability, while smart contract logic enhances system robustness and accountability.

Table 3. Benefits and Obstacles of blockchain.

Benefits	Obstacles
Distributed	Capacity for growth
Unchangeable	Limited interoperability
Clarity and Traceability	Compromise of privacy
Data reliability and privacy	Elevated energy usage
Access of data is authorized	Insufficient technical expertise
Confidence	Creating optimized smart contracts

5.Integrating Federated Learning and Blockchain in Healthcare Applications

Implementing federated learning and blockchain technologies in healthcare offers significant advantages for secure storage, sharing, and utilization of medical data. During the COVID-19 pandemic, disseminating reliable and accurate information became crucial, leading several researchers to develop models combining these technologies (Kumar et al., 2020).

These integrated approaches enabled secure sharing of COVID- 19 patient data among multiple

hospitals while preserving data confidentiality (Rahman et al., 2020, pp. 205071-205087). This methodology extended beyond pandemic crisis management to encompass broader healthcare frameworks.

Several research teams devoted themselves to developing stable healthcare frameworks integrating federated learning and blockchain technologies. These frameworks primarily aimed at protecting the privacy of data from Internet of Health Things (IoHT) devices (Dwivedi et al., 2019, p326) and developing Internet of Medical Things (IoMT) solutions.

Recognizing the vast potential of these technologies, we have incorporated them into a framework for the healthcare sector, as illustrated in **Figure 5**.

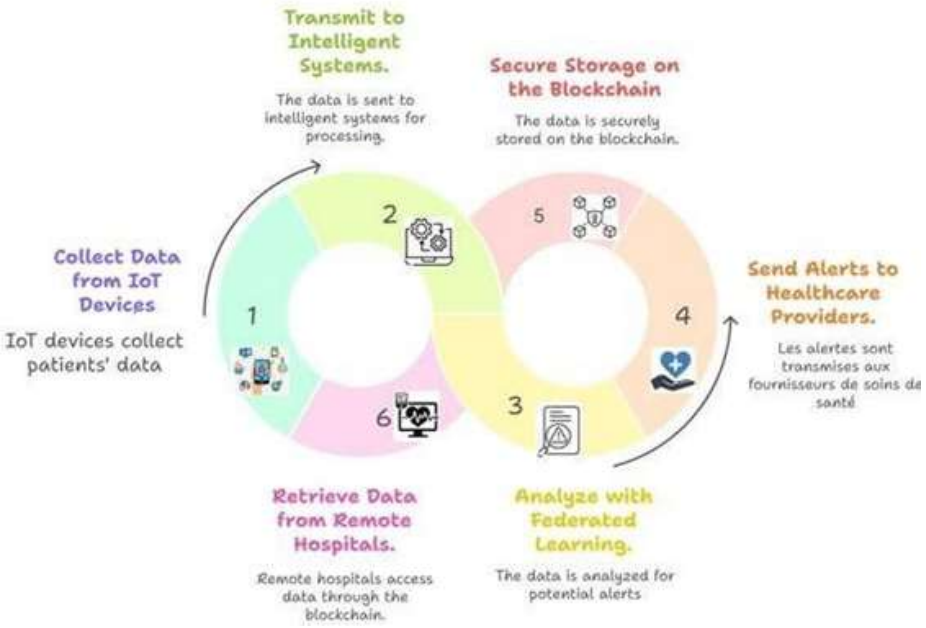

Fig5. Health Data Security Cycle.

The proposed framework demonstrates the integration of blockchain and federated learning with the Internet of Things in medical domain (IoMT).

In this architecture, IoT devices such as medical sensors (blood pressure monitors, glucose meters, insulin pumps, and other patient-connected devices) **[47]** generate raw data and transmit them to IoT devices. These devices then transmit the data to intelligent systems such as smart monitors, laptops, and mobile devices, which possess processing capabilities like translation and compression.

This data is subsequently sent to a blockchain and federated learning-based distributed network. Blockchain ensures security and privacy through a decentralized approach and maintains a tamper-resistant ledger. Federated learning analyzes the data and transmits an alert to the intelligent system in case of a problem, this alert being transferred to the healthcare provider without adding a block in the blockchain network.

This case study has shown that federated learning coupled with blockchain could be useful in preserving privacy in smart healthcare systems. With the combination of these technologies, the safety of medical data transfer and storage is guaranteed, and, simultaneously, the data analysis becomes efficient. Remote hospitals can now access patient clinical records and model aggregate updates, which promote privacy-preserving collaborative healthcare delivery, through blockchain.

The distant hospitals can retrieve patient clinical information and global model updates through blockchain.

Motivations

Traditional centralized data storage methods pose risks related to sensitive patient information, making it imperative to explore innovative solutions that prioritize both data integrity and patient confidentiality. That is why, we are encouraged to study the benefits of federated or collaborative learning which prevents data sharing and the advantages of blockchain technologies which remedies the problem of centralization and guarantees data security in the healthcare sector, especially in the IoMT environment. Moreover, the motivation to adopt these technologies is underscored by the potential for improved healthcare outcomes. By leveraging the capabilities of blockchain and federated learning, healthcare systems can enable more precise predictive analytics, enhancing clinical decision-making and streamline operations.

6.Discussion

we can present our discussion in the form of these points:

1. Challenges in implementing blockchain and federated learning:
    - Integration complexity: Integrating federated learning and blockchain into existing healthcare IT. infrastructures can be complex and resource-intensive.
    - Scalability concerns: The scalability of blockchain solutions remains a concern, particularly in environments with a high volume of transactions.
    - Need for standardized protocols: there is an urgent requirement for uniform procedures and interoperability frameworks to enable seamless communication among diverse IoMT sensors and systems.
    - Too much central-client communication.
    - Cost of time and precision
2. Potential benefits of federated learning and blockchain in medical sector:
    - Improving information confidentiality and protection
    - Enhancing collaboration plus the exchange of data among healthcare providers.
    - Streamlining clinical trials and drug development processes
    - Enabling real-time monitoring and personalized treatment plans.
    - Reducing administrative costs and improving efficiency in healthcare operations.

7. Conclusion

The combination of federated learning and blockchain has become a paradigm shift in healthcare system, namely the Internet of Medical Things. Federated learning allows training machine learning models collaboratively, but sensitive patient data stays local and secure, which is why its development is now seen as a response to the increasing concerns regarding the confidentiality of data. Simultaneously, blockchain provides a transparent, tamper- resistant, and audit system to manage and oversee medical information and transactions to improve the trust of the stakeholders. These technologies combine to create a privacy- conscious and decentralized ecosystem, which enhances the efficiency and security of delivering healthcare services. With continued growth of IoMT, the convergence between federated learning and blockchain will be extremely significant in enhancing data-driven healthcare and preserving the patient trust, privacy, and legal adherence. As is highlighted in this review, their joint potential lies in redeveloping the future of healthcare systems via secure, collaborative and innovative solutions.

References

- Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain technology in healthcare: A systematic review. *Healthcare, 7*(2), 56. https://doi.org/10.3390/healthcare7020056
- Aich, S., et al. (2022). Protecting personal healthcare record using blockchain & federated learning technologies. In *2022 24th International Conference on Advanced Communication Technology (ICACT)* (pp. xxx–xxx). IEEE.
- Akkaoui, R., Hei, X., & Cheng, W. (2020). EdgeMediChain: A hybrid edge blockchain-based framework for health data exchange. *IEEE Access, 8*, 113467–113486.
- Al Asqah, M., & Moulahi, T. (2023). Federated learning and blockchain integration for privacy protection in the Internet of Things: Challenges and solutions. *Future Internet, 15*(6), 203. https://doi.org/10.3390/fi15060203
- Alpaydin, E. (2020). *Introduction to machine learning* (4th ed.). MIT Press.
- Ali, M. S., et al. (2018). Applications of blockchains in the Internet of Things: A comprehensive survey. *IEEE Communications Surveys & Tutorials, 21*(2), 1676–1717.
- Bagdasaryan, E., et al. (2020). How to backdoor federated learning. In *Proceedings of the 23rd International Conference on Artificial Intelligence and Statistics (AISTATS)* (pp. xxx–xxx). PMLR.
- Bernabe, J. B., et al. (2019). Privacy-preserving solutions for blockchain: Review and challenges. *IEEE Access, 7*, 164908–164940.
- Brogan, J., Baskaran, I., & Ramachandran, N. (2018). Authenticating health activity data using distributed ledger technologies. *Computational and Structural Biotechnology Journal, 16*, 257–266.
- Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics, 36*, 55–81.
- Casola, V., et al. (2016). Healthcare-related data in the cloud: Challenges and opportunities. *IEEE Cloud Computing, 3*(6), 10–14.
- Christ, M. J., et al. (2019). Exploring blockchain in healthcare industry. In *2019 International Conference on ICT for Smart Society (ICISS)* (pp. xxx–xxx). IEEE.
- Dai, H.-N., Zheng, Z., & Zhang, Y. (2019). Blockchain for Internet of Things: A survey. *IEEE Internet of Things Journal, 6*(5), 8076–8094.
- Dasaklis, T. K., Casino, F., & Patsakis, C. (2018). Blockchain meets smart health: Towards next generation healthcare services. In *2018 9th International Conference on Information, Intelligence, Systems and Applications (IISA)* (pp. xxx–xxx). IEEE.
- Donawa, A., Orukari, I., & Baker, C. E. (2019). Scaling blockchains to support electronic health records for hospital systems. In *2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)* (pp. xxx–xxx). IEEE.
- Dwivedi, A. D., et al. (2019). A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors, 19*(2), 326.

- El Khediri, S. (2025). Secure IoT healthcare: Federated learning and blockchain for privacy-preserving AI. In *International Conference on Computational Collective Intelligence*. Springer Nature Switzerland.
- Ghosh, P. K., et al. (2023). Blockchain application in healthcare systems: A review. *Systems, 11*(1), 38.
- Hewa, T., Ylianttila, M., & Liyanage, M. (2021). Survey on blockchain-based smart contracts: Applications, opportunities and challenges. *Journal of Network and Computer Applications, 177*, 102857.
- Hiwale, M., Phanasalkar, S., & Kotecha, K. (2021). Using blockchain and distributed machine learning to manage decentralized but trustworthy disease data. *Science & Technology Libraries, 40*(2), 190–213.
- Hussain, I., Young, S., & Park, S.-J. (2021). Driving-induced neurological biomarkers in an advanced driver-assistance system. *Sensors, 21*(21), 6985.
- Kang, M., et al. (2018). Recent patient health monitoring platforms incorporating Internet of Things-enabled smart devices. *International Neurourology Journal, 22*(Suppl. 2), S76.
- Kuo, T.-T., Kim, H.-E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association, 24*(6), 1211–1220.
- Kumar, R., et al. (2020). Blockchain-federated-learning and deep learning models for COVID-19 detection using CT imaging. *arXiv preprint arXiv:2007.06537*.
- Li, H., et al. (2023). Review on security of federated learning and its application in healthcare. *Future Generation Computer Systems, 144*, 271–290.
- Li, P., et al. (2019). ChainSDI: A software-defined infrastructure for regulation-compliant home-based healthcare services secured by blockchains. *IEEE Systems Journal, 14*(2), 2042–2053.
- McMahan, B., et al. (2017). Communication-efficient learning of deep networks from decentralized data. In *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS)* (pp. xxx–xxx). PMLR.
- Mershad, K., & Cheikhrouhou, O. (2023). Lightweight blockchain solutions: Taxonomy, research progress, and comprehensive review. *Internet of Things, 24*, 100984.
- Motohashi, T., et al. (2019). Secure and scalable mHealth data management using blockchain combined with client hashchain: System design and validation. *Journal of Medical Internet Research, 21*(5), e13385.
- Mothukuri, V., et al. (2021). A survey on security and privacy of federated learning. *Future Generation Computer Systems, 115*, 619–640.
- Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf
- Ndayizigamiye, P., & Dube, S. (2019). Potential adoption of blockchain technology to enhance transparency and accountability in the public healthcare system in South Africa. In *2019 International Multidisciplinary Information Technology and Engineering Conference*

(IMITEC) (pp. xxx–xxx). IEEE.

- Pandl, K. D., et al. (2020). On the convergence of artificial intelligence and distributed ledger technology: A scoping review and future research agenda. *IEEE Access, 8*, 57075–57095.
- Patel, A. D., et al. (2024). Security trends in Internet-of-Things for ambient assistive living: A review. *Recent Advances in Computer Science and Communications, 17*(7), 18–46.
- Rahman, M. A., et al. (2020). Secure and provenance enhanced Internet of Health Things framework: A blockchain-managed federated learning approach. *IEEE Access, 8*, 205071–205087.
- Rieke, N., et al. (2020). The future of digital health with federated learning. *NPJ Digital Medicine, 3*(1), 119.
- Singh, S., et al. (2020). Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. *Sustainable Cities and Society, 63*, 102364.
- Tomaz, A. E. B., et al. (2020). Preserving privacy in mobile health systems using non-interactive zero-knowledge proof and blockchain. *IEEE Access, 8*, 204441–204458.
- Tripathi, G., Ahad, M. A., & Paiva, S. (2020). S2HS: A blockchain-based approach for smart healthcare system. *Healthcare, 8*(1), 100.
- Ulhaq, A., & Burmeister, O. (2020). COVID-19 imaging data privacy by federated learning design: A theoretical framework. *arXiv preprint arXiv:2010.06177*.
- Wang, X., et al. (2020). Convergence of edge computing and deep learning: A comprehensive survey. *IEEE Communications Surveys & Tutorials, 22*(2), 869–904.
- Xu, J., et al. (2021). Federated learning for healthcare informatics. *Journal of Healthcare Informatics Research, 5*, 1–19.
- Yazdinejad, A., et al. (2020). Decentralized authentication of distributed patients in hospital networks using blockchain. *IEEE Journal of Biomedical and Health Informatics, 24*(8), 2146–2156.
- Zheng, Z., et al. (2020). An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems, 105*, 475–491.