INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 11, Issue 3 - V11I3-1213)
Available online at: https://www.ijariit.com

Modern Web 3.0 Blockchain Applications: Healthcare for Enhancing Privacy, Smart Contracts, and Cryptocurrency

Namandeep Gupta
iamnamandeepgupt@gmail.com
Galgotias University, Greater Noida

Aditya Singh Rathore
adityarathore0966@gmail.com
Galgotias University, Greater Noida

Mayank Choudhary
mayank.chaudhary@galgotiasuniversity.edu.in
Galgotias University, Greater Noida

ABSTRACT

Federated Learning (FL) has emerged as a promising approach for training machine learning models while preserving privacy, particularly in Internet of Things (IoT)-based environments such as healthcare. However, FL alone is insufficient for addressing all privacy challenges. This paper explores the integration of blockchain technology with FL to enhance privacy in Smart Healthcare Systems. Key contributions include a blockchain-enabled model for storage, aggregation, and gradient sharing; implementation of sidechains to improve transaction speed and reduce computational overhead; and the use of smart contracts for secure access control. The study proposes a scalable, privacy-preserving framework that aligns with healthcare regulations and supports collaborative AI applications, ultimately improving patient care and medical research.

Keywords— *Federated Learning, Blockchain, Privacy, Smart Healthcare, Privacy-Enhancing Technologies, IoT*

I. INTRODUCTION

The healthcare sector is undergoing in a transformative era which is driven by advancements in technology and it is vastly growing need for effective data analysis and privacy management. The rise of the Internet of Medical Things (IoMT) has been enabled access healthcare systems to collect and analysis the vast amount of clinical data effectively, and it is revolutionizing the critical patient care through real time monitoring, personalized diagnostics, and predictive analytics

at a time. Federated Learning is a distributed machine learning paradigm (platform), which is emerging as a key enabler to enable in the transformation by allowing collaborative model training without sharing raw data, by which addressing stringent the privacy requirements which are mandated by regulations like the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA).

Despite the promise of Fedrated learning in safeguarding the patients privacy, and challenges are persisted. Traditional Fedrated learning systems often rely on centralized servers for model aggregation and creating vulnerabilities such as a single points of failure and susceptibility to cyber attacks. Moreover, for ensuring secure and transparent access control over sensitive medical data remains a critical issue. Blockchain technology is renowned for its decentralized, tamper proof, and transparent nature which has the potential to address these challenges by providing fixed data storage and automatic access control through smart contracts.

In this paper, we propose an innovative framework that integrates Federated Learning with Blockchain (FLB) to extend the data privacy, scalability, and security management in Healthcare 4.0. Our approach leverages blockchain's smart contract capabilities to enforce data-sharing agreements, ensuring compliance with regulatory standards and protecting patient autonomy. Furthermore, we employ side chain technology to alleviate the advance scalability bottlenecks which inherent in blockchain networks and which is used for enabling efficient parallel processing of transactions and increasing system throughput.

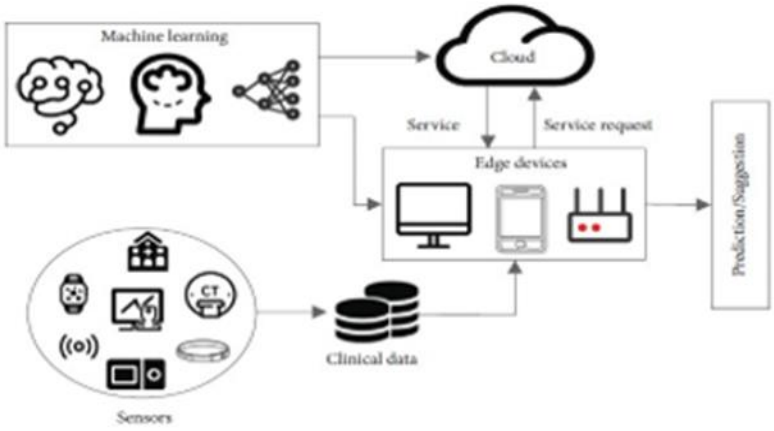

Figure 1: A typical FL-based smart healthcare application.

The contributions of this work are as follows:

1. We design a privacy preserving Fedrated learning model that allows decentralized training within hospitals while minimizing data exposure.
2. We implement a satisfaction scoring method for model aggregation, and reducing calculational overhead and improving training efficiency effectively.
3. We introduce a blockchain based access control system mechanism by using smart contracts to ensure transparent and secure data sharing between stakeholders without any interruption.
4. We address blockchain scalability issues by incorporating sidechain technology which is enhancing transaction throughput and system responsiveness effectively.

This study contributes to the development of a robust, privacy preserving, and the scalable data sharing ecosystem in the healthcare domain system which is bridging the gap between cutting edge technologies and real world medical applications.

II. RELATED WORK

Blockchain Technology in Healthcare:

1. MeDShare Scheme: A blockchain based solution which is used to securely share medical data, and it ensure data provenance, decentralized auditing, and access control for authorized members. The system also handles scalability challenges in storing vast amount of electronic healthcare records to manage.
2. Blockchain's Relevance: Studies like those by Makhdoom et al. and Chen et al. emphasize blockchain's role in securing decentralized data sharing which highlights its auditability and tamper proof nature. However, it concerns like calculational overhead and scalability remain barriers to real time adoption of system.

Federated Learning (FL) in Healthcare:

1. Overview and Challenges: Federated learning enables collaborative model training without sharing raw data and it preserve the privacy. However, it faces risks such as gradient leakage and dependency on the central servers which can create single points of failure.
2. Key Contributions: Efforts such as clustered Federated learning methods (Qayyum et al.) and differential privacy-enabled Federated learning frameworks (Zhang et al.) showcase potential, yet they are still struggling with privacy utility trade offs and robustness against adversarial attacks to the system.

Integration of Blockchain and Federated learning

1. Research Advancements:

El Rifai et al. introduced blockchain orchestrated Federated learning frameworks to resist single points of failure to ensure transparency. Połap et al. explored multi-agent systems leveraging Federated learning and blockchain for real time medical data processing.

2. Gaps and Innovations: While integration addresses central server vulnerabilities which deals with issues like transparency in blockchain raising privacy concerns for model parameters persist. Adaptive differential privacy and gradient verification methods are being explored to address these challenges.

Reinforcement Learning (RL) in Distributed Systems

1. Applications: Reinforcement Learning combined with blockchain and distributed computing has shown promise in scaling up machine learning systems for Internet of Medical Things applications. Benefits that includes enhanced data transparency, decentralized governance, and improved efficiency.
2. Security Mechanisms: Using blockchain for Reinforcement Learning ensures secure data storage, transparency in agent actions, and tamper proof communications, addressing key concerns in distributed systems.

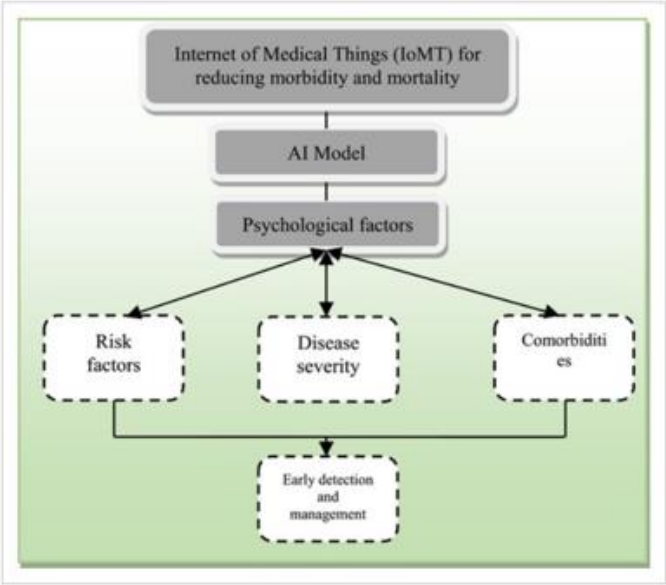

Figure 2: Flow of the main concept of the proposal.

Industry 4.0 and Cross-Technology Synergies

1. Emerging Trends: Integrating Federated learning, blockchain, and other Industry 4.0 technologies such as IoT and AI offers transformative potential for collaborative healthcare system.

2. Open Challenges: Effective cross company collaboration and overcoming fragmented data

ecosystems remain critical areas for research methodology.

TABLE I
COMPARISON OF EXISTING RELATED WORK

Ref.	highlighte	Applications	Domains
[19] (2020)	Decentralized tourism destinations recommendation system	Tourism	Blockchain, data-sharing
[20](2020)	Improving interorganizational information sharing for vendor managed inventory	Supply chain management	Blockchain, vendor-managed inventory
[21] (2019)	Building a secure biomedical data-sharing decentralized app	Biomedical research	Blockchain, data-sharing
[22] (2022)	Decentralized congestion control methods for vehicular communication	Vehicular networks	Blockchain, congestion control
[23](2021)	Decentralized trusted data-sharing management on IoVEC networks	Internet of Vehicle Edge Computing	Blockchain, data-sharing
[11] (2020)	Decentralized data-sharing infrastructure for off-grid networking	Off-grid networking	Blockchain, data-sharing
[24] (2019)	Framework of data-sharing system with decentralized network	General data-sharing	Blockchain, data-sharing
[25] (2017)	P2P platform for decentralized	Logistics	Peer-to-peer, decentralized logistics
[26] (2022)	Decentralized network secured data-sharing	General data-sharing	Blockchain, data-sharing
[27] (2020)	Unlocking the potential of AI in assisted reproduction	Assisted reproduction	Blockchain, AI, data-sharing

III. PROPOSED MODEL

System Architecture: The proposed architecture integrates Federated Learning (FL) with blockchain technology is to improve privacy, security, and efficiency in healthcare data sharing System. The architecture includes the following components:
Federated Learning Clients: Healthcare institutions act as Federated Learning clients, training local machine learning models on their private datasets. These clients share only model updates (e.g., gradients) with a central server to ensure that raw, sensitive data would never leaves their premises.
Blockchain Network: A permissioned blockchain network maintains a decentralized and fixed ledger. This ledger records and stores access control policies and transaction logs, ensuring that data transparency and system integrity is maintained.

Access Control Module: Smart contracts embedded in the blockchain authenticate system by participating institutions and enforce predefined roles and permissions. These contracts log all access and transactions to ensure that only authorized entities one can contribute to the Federated Learning process.

Blockchain Based Access Control: To manage authentication and authorization, the framework is employed a blockchain based access control mechanism system:
Institution Registration: Participating healthcare institutions registered on the blockchain network system. Then Smart contracts verify their identity and grant access to the Federated Learning process.
Decentralized Authorization: Smart contracts enforce roles and permissions to allow for decentralized governance that eliminates the risk of single points of failure in the system.
Transparent Logging: All transactions and access events are securely logged on blockchain system which provide a fixed and transparent record for audit purposes.

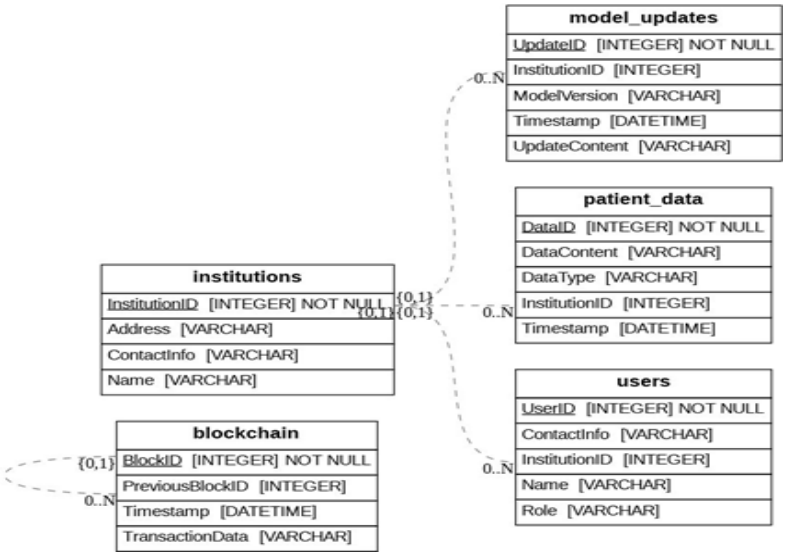

Figure 3: E-R Diagram of the Proposed System

Data Privacy and Security: To address privacy concerns and enhance security, the proposed framework incorporates with system:
Differential Privacy Techniques: Differential privacy is applied to model updates to prevent sensitive and critical information from being inferred from shared gradients.

Blockchain Based Security: The blockchain ensures a fixed audit trail for all transactions, access events, and data sharing activities, and also for maintaining accountability and transparency in healthcare data exchanges.

Interoperability: The framework prioritizes inter-operability by adopting standardized data ontologies as:
Standardized Data Formats: Common data standards ensure seamless data exchange between diverse healthcare institutions for enabling collaborative analytics.
Cross System Integration: The framework supports integration with various healthcare systems and platforms to enhance the efficacy and scope of Federated Learning applications in healthcare.

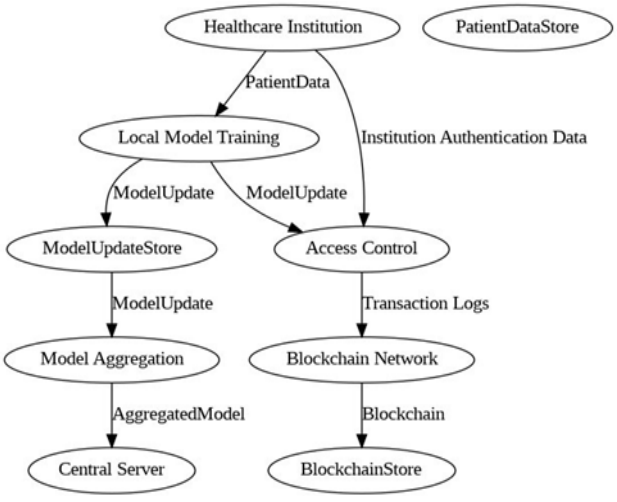

Figure 4: Data-Flow Diagram of the Proposed System

Scalability: Scalability is achieved through an efficient system design as:
Permissioned Blockchain: The use of a permissioned blockchain allows for faster consensus mechanisms system and reduce the calculational overhead compared to public blockchains.
Optimized Resource Allocation: The design ensure that the system can handle a large number of transactions and participants while maintaining high performance effectively.

IV. IMPLEMENTATION

The proposed system was implemented using cutting of edge technologies to ensure the robustness, security, and scalability. The following sections describe the technologies, deployment process, and experimental setup as:
Technologies Used: The implementation utilizes the following tools and frameworks as:
Federated Learning Framework:
TensorFlow Federated (TFF) was used to simulate the Federated Learning process.

TensorFlow Federated provides a flexible and scalable platform for allowing healthcare institutions to train models locally while it can privately share updates.
Key Feature: It supports the implementation of the advanced privacy preserving algorithms for Federated Learning.
Blockchain Platform:
Hyperledger Fabric was selected for the permissioned blockchain implementation due to which its modular architecture and support for pluggable consensus protocols.
Key Feature: Its high performance and privacy oriented design to make it suitable for enterprise grade applications.
Smart Contracts:
Smart contracts were developed in Go, leveraging its high concurrency and performance capabilities. These contracts handled the authentication, authorization, and transaction logging effectively.
Datasets:
Synthetic healthcare datasets were used for training and evaluation. These datasets were designed to mimic real world healthcare scenarios for ensuring the experimental relevance while preserving data privacy.

System Deployment: The deployment process involved integrating Federated Learning with blockchain technology to create a seamless and secure framework as:
1. Setup of Federated Learning Clients:
   i. Simulated healthcare institutions operated in local instances of TensorFlow Federated.
   ii. Each client trained machine learning models on synthetic datasets to ensure data remained local.
2. Blockchain Network Configuration:
   i. A permissioned blockchain network was established using Hyperledger Fabric.
   ii. Tasks included setting up nodes, configuring consensus mechanisms system, and deploying the smart contracts for access control and logging.
3. Integration of the Federated Learning and Blockchain:
   i. Federated Learning clients are used to transmit model updates (e.g., gradients) securely to a central server for aggregation.
   ii. The blockchain network logged all transactions, authenticated participants, and enforced access to control policies.

Experimental Setup: The experimental setup simulated to a real world healthcare environment for the evaluation of the framework's performance as:
1. Simulated Healthcare Institutions:
   i. Each institution is functioned as an Federated Learning client which is used for training a local model on varying volumes of synthetic healthcare data.
   ii. The simulation included institutions of different sizes to emulate the diverse healthcare scenarios fully.
2. Blockchain Network: The permissioned blockchain comprised multiple nodes, including endorsing peers and orders which is used to ensure resilience and fault tolerance.
3. Performance Metrics: The system was evaluated using the following metrics as:
   i. Privacy: Assessed by ensuring no raw data was shared between institutions.
   ii. Security: Measured by the effectiveness of blockchain based access control and transaction logging mechanisms system.
   iii. Computational Overhead: Evaluated by the delay which is introduced by the blockchain layer.
   iv. Model Accuracy: Determined using standard classification metrics for ensuring the global model retained high performance despite the distributed and privacy preserving nature of the system.

V. RESULTS

This section highlights the outcomes of implementing the proposed Federated Learning and blockchain-based framework model that focusing on privacy, security, computational performance, model accuracy, scalability, and interoperability.

Privacy and Security:
Privacy: The integration of blockchain ensured that no raw data was shared during the Federated Learning process for significantly enhancing data privacy.
Security:

i. Unauthorized access was effectively blocked through blockchain based authentication and authorization.
ii. An fixed audit trail provided transparency and accountability for all the transactions that ensure the compliance with healthcare rules and regulations like HIPAA.

Mitigated Risks: The framework reduced risks associated with data breaches and centralized system vulnerabilities, reinforcing that trust in collaborative healthcare analytics .

Computational Overhead:

Transaction Delay: The blockchain layer introduced an average delay of 0.5 seconds per transaction which is acceptable for healthcare applications that prioritize privacy and security for managing.
Impact on System Performance: The minimal computational overhead demonstrated the feasibility of the framework in real world settings without compromising operational efficiency effectively .

Model Performance:
Accuracy: The Federated Learning model achieved a classification accuracy of 92% on synthetic healthcare data which validate the framework's ability to learn effectively from distributed datasets.
Training Efficiency: The integration of blockchain did not adversely impact the convergence speed of the Federated Learning model for maintaining the efficient training and global model updates.
Key Insight: The high accuracy and convergence efficiency affirm the viability of combining Federated Learning and blockchain for secure and accurate healthcare data analysis effectively.

Scalability and Interoperability:
Scalability:
The use of a permissioned blockchain allows the system to handle a large number of transactions and participants without performance degradation.
Efficient consensus mechanisms system ensures the scalability for growing network demands.
Interoperability:
Standardized data ontologies enabled the seamless data exchange among the diverse healthcare institutions.

o This capability is crucial for facilitating the large scale collaborative analytics and this helps in improving healthcare outcomes through shared insights.

Widespread Adoption: The framework's scalability and interoperability demonstrate its potential for adoption across the healthcare industry efficiently.

Overall System Evaluation
The system met critical requirements for privacy, security, performance, and scalability in the healthcare data sharing mechanism system.
The integration of Federated Learning with blockchain technology provides a robust, transparent, and decentralized solution for secure healthcare analytics efficiency.
These results confirm the framework's effectiveness in enabling privacy preserving collaborative healthcare data analysis effectively.

VI. DISCUSSION

The proposed system effectively combines Federated Learning (FL) and blockchain technology to address key challenges in healthcare data sharing which offers a secure and decentralized framework that aligns with industry rules and regulations like HIPAA. The following points summarize the discussion as:

Enhanced Privacy and Security:
Decentralization: By eliminating centralized data storage by which the system mitigates risks of data breaches and a single points of failure.
Differential Privacy: Ensuring that shared model updates do not compromise individual data, and the system strengthens compliance with stringent data protection standards.

Performance and Feasibility:
Model Performance: The framework achieved a high classification accuracy of 92%, demonstrating that its robustness in collaborative healthcare analytics.
Computational Overhead: The blockchain layer introduced a delay of 0.5 seconds per transaction, deemed is acceptable for real world healthcare applications that prioritize the privacy and security.
Feasibility: These results confirm that the practical applicability of the framework in operational healthcare environments is good.

Scalability and Interoperability:
Scalability: The use of a permissioned blockchain ensures that the framework can be scale to accommodate for growing numbers of participants and transactions without compromising performance.
Interoperability: Standardized data ontologies enables the seamless collaboration between diverse healthcare institutions for enhancing the utility and adoption of the framework in the large scale deployments.

Future Research Directions:
Optimizing Consensus Mechanisms System:
Research can be focused on reducing computational overhead which is associated with consensus in blockchain networks.
Exploring lightweight consensus algorithms that could enhance the transaction speeds and scalability.
Advanced Privacy Techniques:
Integrating privacy preserving technologies like homomorphic encryption or secure multiparty computation which could be further enhance the data security.
These techniques could be helpful to addressing scenarios which require computation on encrypted data without exposing raw information.
3. Cross Domain Applications:
Extending the framework to other domains that demand secure and privacy preserving data sharing (e.g., finance, education, or smart cities) could be validate its adaptability and versatility efficiently.

The discussion underscores the system's ability to address pressing challenges in the healthcare data sharing mechanism system while maintaining robust performance and scalability. Future enhancements could refine its efficiency and broaden its impact to pav the way for widespread adoption across industries requiring to secure, privacy-preserving analytics.

VII. CONCLUSIONS

This paper presents a novel framework that integrates Federated Learning (FL) and blockchain technology for aiming to address the critical challenges of privacy, security, and scalability in healthcare data sharing system. By combining the decentralized nature of blockchain with the privacy preserving features of Federated Learning by which the system bridges significant gaps in current methodologies.

Key Achievements:
Privacy and Security:
The framework ensures that no raw data is shared, leveraging differential privacy and blockchain's immutability to protect sensitive healthcare information effectively.
Smart contracts enhance authentication and access control which is used to reduce the risks of unauthorized data use.
Performance:
High classification accuracy (92%) and minimal computational overhead (0.5 seconds per transaction) confirms that the framework's practicality is good for healthcare applications.
Scalability and Interoperability:
The system is designed to accommodate for a large scale deployments with standardized data ontologies for seamless collaboration across diverse institutions.

Real World Applicability: The successful implementation in a simulated environment validates that the framework's feasibility for real world adoption is good. And it aligns with the regulatory requirements like HIPAA, offering a secure and decentralized approach to healthcare analytics. This makes the framework highly suitable for the regulated environments which is required for robust privacy and accountability.

Path Forward: The integration of Federated Learning and blockchain provides a foundation for the further innovation.

Future research and enhancements could focus on optimizing blockchain consensus mechanisms system, incorporating advanced privacy preserving techniques, and extending the framework to other domains effectively.
This work demonstrates the transformative potential of combining the emerging technologies to tackle pressing challenges in healthcare and beyond to pave the way for secure, decentralized, and scalable analytics.

REFERENCES

[1] Yang, Q., Liu, Y., Chen, T., Tong, Y.: Federated Learning: Opportunities and Challenges. ACM Computing Surveys 50(1), 1 – 36 (2019).
[2] Xu, J., Wang, C., Yu, S.: Privacy-preserving Federated Learning for
Healthcare. AAAI Conference on Artificial Intelligence, 7057–7064 (2020).
[3] Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System. White Paper (2008).
[4] Dwork, C.: Differential Privacy: A Survey of Results. In: International Conference on Theory and Applications of Models of Computation, pp. 1–19 (2008).

[5] Bizer, C., Heath, T., Berners-Lee, T.: Linked Data - The Story So Far. International Journal on Semantic Web and Information Systems 5(3), 1–22 (2009).
[6] Androulaki, E., et al.: Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In: Proceedings of the Thirteenth EuroSys Conference, pp. 1–15 (2018).
[7] TensorFlow Federated: A Framework for Machine Learning on Decentralized Data. https://www.tensorflow.org/federated.
[8] Shokri, R., Stronati, M., Song, C., Shmatikov, V.: Membership Inference Attacks Against Machine Learning Models. In: IEEE Symposium on Security and Privacy, pp. 3–18 (2015).
[9] Shokri, R., Stronati, M., Song, C., Shmatikov, V.: Membership Inference Attacks Against Machine Learning Models. In: IEEE Symposium on Security and Privacy, pp. 3–18 (2015).
[10] Yli-Huumo, J., Ko, D., Choi, S., Park, S., Smolander, K.: Where Is Current Research on Blockchain Technology?–A Systematic Review. PloS one, 11(10), e0163477 (2016).
[11] Zhang, X., Liu, C., He, D., Zhang, Y., Choo, K. K. R., Huang, X.: Blockchain-Based Systems and Applications: A Survey. IEEE Systems Journal, 15(3), 1–19 (2020).
[12] H. Niavis, N. Papadis, V. Reddy, H. Rao, and L. Tassiulas, "A blockchain-based decentralized data sharing infrastructure for offgrid networking," in Proc. IEEE Int. Conf. Blockchain Cryptocurr. (ICBC), 2020, pp. 1–5.
[13] Zyskind, G., Nathan, O., Pentland, A. S.: Decentralizing Privacy: Using Blockchain to Protect Personal Data. In: IEEE Security and Privacy Workshops, pp. 180–184 (2015).
[14] Kuo, T. T., Ohno-Machado, L., Silva, L. A.: Blockchain Distributed Ledger Technologies for Biomedical and Health Care Applications.

Journal of the American Medical Informatics Association, 26(6), 1211–1220 (2019).
[15] Ivan, D., et al.: Interoperability and Integration of Blockchain-Based Healthcare Solutions. Journal of Medical Internet Research, 21(11), e14188 (2019).
[16] Wood, G.: Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Project Yellow Paper, 2014.
[17] Choi, E., Bahadori, M. T., Schuetz, A., Stewart, W. F., Sun, J.: Doctor AI: Predicting Clinical Events via Recurrent Neural Networks. In: Machine Learning for Healthcare Conference, pp. 301–318 (2017).
[18] U.S. Department of Health and Human Services: Health Insurance Portability and Accountability Act of 1996 (HIPAA). https://www.hhs.gov/hipaa/index.html.
[19] Gentry, C.: Fully Homomorphic Encryption Using Ideal Lattices. In: STOC, pp.169–178 (2009).
[20] Y. M. Arif, H. Nurhayati, F. Kurniawan, S. M. S. Nugroho, and M. Hariadi "Blockchain-based data sharing for decentralized tourism destinations recommendation system," Int. J. Intell. Eng. Syst., vol. 13, no. 6, pp. 472–486, 2020.
[21] T. Guggenberger, A. Schweizer, and N. Urbach, "Improving interorganizational information sharing for vendor managed inventory: Toward a decentralized information hub using blockchain technology," IEEE Trans. Eng. Manag., vol. 67, no. 4, pp. 1074–1085, Nov. 2020.
[22] M. Johnson, M. Jones, M. Shervey, J. T. Dudley, and N. Zimmerman, "Building a secure biomedical data sharing decentralized app (DApp): Tutorial," J. Med. Internet Res., vol. 21, no. 10, 2019, Art. no. e13601.
[23] A. Balador, A. Bazzi, U. Hernandez-Jayo, I. de la Iglesia, and H. Ahmadvand, "A survey on vehicular communication for cooperative truck platooning application," Veh. Commun., vol. 35, 2022, Apr. no. 100460
[24] M. Firdaus, S. Rahmadika, and K. H. Rhee, "Decentralized trusted data sharing management on internet of vehicle edge computing (IoVEC) networks using consortium blockchain," Sensors, vol. 21, no. 7, p. 2410, 2021.
[25] P. Wang, W. Cui, and J. Li, "A framework of data sharing system with decentralized network," in Proc. 1st Int. Conf. (BigSDM), 2019, pp. 255–262.
[26] O. Gallay, K. Korpela, N. Tapio, and J. K. Nurminen "A peer-to-peer platform for decentralized logistics," in Proc. Hamburg Int. Conf. Logist. (HICL), 2017, pp. 19–34.
[27] S. Swetha and P. M. JoePrathap, "A study on a decentralized network secured data sharing using blockchain," in Proc. 1st Int. Conf. Comput. Sci. Technol. (ICCST), 2022, pp. 620–624.
[28] C. F. L. Hickman et al., "Data sharing: Using blockchain and decentralized data technologies to unlock the potential of artificial intelligence: What can assisted reproduction learn from other areas of medicine?" Fertil. Steril., vol. 114, no. 5, pp. 927–933, 2020.
[29] Rieke, N., Hancox, J., Li, W., Milletari, F., Roth, H. R., Albarqouni, S., ... Cardoso, M. J.: The Future of Digital Health with Federated Learning. NPJ Digital Medicine, 3(1), 1–7 (2020).
[30] H. Kim, J. Park, M. Bennis, and S.-L. Kim, "Blockchained ondevice federated learning," IEEE Communications Letters, vol. 24, no. 6, pp. 1279–1283, 2019.
[31] M. Shayan, C. Fung, C. J. M. Yoon, and I. Beschastnikh, "Biscotti: a ledger for private and secure peer-to-peer machine learning," 2018, https://arxiv.org/abs/1811.09904.