Grenze International Journal of Engineering and Technology, January Issue

A Survey Paper on Enhancing Privacy and Security in Decentralized Healthcare with Federated Learning and Blockchain

Priti Shukla[1] and Sachin Patel[2]
[1-2]SAGE University/CSE, Indore, India
Email: priti.svits@gmail.com, drsachinpatel.sage@gmail.com

***Abstract*— This paper explores how combining these two technologies can enhance privacy and security in decentralized healthcare environments. By integrating Federated Learning and Blockchain, it is possible to create a system where data privacy is maintained, patient consent is enforced, and the integrity of medical records is assured. This approach promises to empower healthcare providers and patients alike, enabling more efficient, secure, and trustworthy healthcare systems. The goal of this research is to analyze the potential benefits and challenges of employing Federated Learning and Blockchain in decentralized healthcare, providing insights into how these technologies can reshape the future of medical data management, privacy, and security. In this context, two emerging technologies — Federated Learning (FL) and Blockchain — offer promising solutions to address these challenges. Federated Learning is a machine learning approach that enables collaborative model training without the need for centralized data sharing. This decentralization of data processing not only preserves patient privacy but also enables more robust and personalized healthcare models. On the other hand, Blockchain, with its immutable and transparent ledger system, ensures secure and traceable transactions of medical records, preventing unauthorized access and tampering.**

***Keywords*— Federated Learning (FL), Blockchain for Healthcare, Decentralized Data Sharing, Privacy-Preserving AI.**

I. INTRODUCTION

The healthcare industry is undergoing a rapid digital transformation, driven by data-centric technologies aimed at optimizing clinical treatment, diagnosis, and care delivery. The increased reliance on electronic health records (EHRs), wearable sensors, and interconnected medical devices presents significant challenges related to privacy, security, and data integrity. Traditional centralized healthcare data storage systems remain highly susceptible to cyberattacks, unauthorized access, and single points of failure, posing serious threats to sensitive patient information. A key challenge in modern healthcare is enabling collaborative medical research and data analysis while complying with stringent privacy regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR). Federated Learning (FL) and Blockchain are two emerging technologies that, when combined, offer a promising solution for decentralized healthcare data sharing. FL enhances data privacy by allowing hospitals, research institutions, and medical organizations to collaboratively develop machine learning models without transferring raw patient data.

Grenze ID: 01.GIJET.12.1.374

This ensures that sensitive medical information remains within local devices while still contributing to the development of a global predictive model. However, FL alone does not address the challenges of secure inter-institutional communication, data integrity, and transparency. Blockchain technology, with its inherent properties of decentralization, immutability, and transparency, complements FL by providing tamper-proof data storage, decentralized identity management, and secure access control. Implementing Hyperledger Fabric for blockchain transactions, InterPlanetary File System (IPFS) for decentralized storage, and smart contracts for automated validation further enhances the security and reliability of healthcare data exchanges. Additionally, techniques such as zero-knowledge proofs (ZKP) and homomorphic encryption introduce advanced privacy-preserving computations, preventing unauthorized access while ensuring secure processing of medical data.

II. LITERATURE REVIEW

Stephanie et al. (2022),In the same vein, the trend of Industry 4.0 initiates the Healthcare 4.0 and introduces IoT-powered medical imaging for the early detection of diseases. But because of privacy concerns and differences in institutional computational capabilities, AI and big data adoption remain behind. To this end, this study introduced a blockchain-based federated learning method to provide secure and collaborative data sharing [1].

Alkhalifa et al. (2024),The Internet of Medical Things (IoMT) integrates various medical devices to enhance patient treatment by facilitating the real-time exchange of information. Privacy-preserving federated learning (PPFL) facilitates collaborative ML training without sending sensitive data. This work proposes the PPFL-BCSHS system, which incorporates blockchain with anomaly detection (i.e., MGO-based feature selection, BiGRU, and SCSO tuning) to improve IoMT's security and performance [2].

Ngoupayou Limbepe et al. (2025),Privacy Preservation in Smart Healthcare Systems with Federated Learning (FL) FL enforces privacy in smart healthcare systems but has certain drawbacks. We present the integration of blockchain and privacyenhancing technologies (PETs) to improve FL frameworks. This survey focuses on blockchain-enabled storage, aggregation and gradient uploads, emphasizing their importance in securing healthcare data and improving trustworthiness in the systems[3].

Bezanjani et al. (2024),IoT revolutionized healthcare, but the tech also brought a kink to cybersecurity challenges. This paper defines a three-phase security model comprised of data transaction encryption through blockchain, access control through pattern recognition and intrusion detection through bi-directional long short-term memory (BiLSTM). Better accuracy, precision and intrusion detection performance was achieved by this method than the existing techniques, which speed and direct the proposed method as accurate[4].

Guduri et al. (2023),To achieve proper safety of electronic health records (EHRs), this research presents a federated learning mechanism with a lightweight blockchain-based encryption scheme. This eliminates the security risk of relying on third parties to gain access to encrypted data, such as OAuth services, For more precious and encrypted data, using Smart Contracts and Proxy Re-encryption technology. Tested using an Ethereum testbed, the model guarantees improved security and outperforms traditional forms of encryption [5].

Alzakari et al. (2024),In this paper, we propose a new methodology that employs Machine Learning (ML)/blockchain/intrusion detection systems (IDS) to advance the security and predictive analytics in the internet of healthcare things (IoHT). This approach incorporates federated learning to safeguard data privacy while facilitating accurate health prediction as well as intrusion detection. Some critical advantages here include improving federated learning with blockchain, IDS-based threat detection, and synchronizing artificial neural networks to achieve high efficacy ratios accounting for 97.75% for intrusion detection and 98% for disease prediction [6].

Khan et al. (2023),While the rapid advances in the Internet of Medical Things (IoMT) have changed the pattern of healthcare, it has also led to security vulnerabilities like replay attack, data tampering and identity spoofing. Advanced Security Framework for Real Time Health Care Applications: Encrypting and Protecting Medical DataAbstract: In the context of health care, protecting real- time medical data before, during, and after transmission is of paramount importance. Our proposed framework achieves substantial enhancements in terms of anomaly detection and resilience towards cyber-based offenses compared to existing solutions such as MRMS and BACKM-EHA (7).

Butt et al. (2023),In the context of COVID-19, federated learning (FL) can be useful to allow organizations to collaboratively train an AI model without sharing any of their data. In this study, a COVID-19 diagnosis using chest X-ray images is accomplished using an FL-based system with the help of localized and fog-computing-based CNN models. The global FL model achieves superior performance compared to local models while

maintaining patient privacy. The study focuses on the combination of AI, FL, and medical imaging to offer better healthcare [8].

Kumar et al. (2024),Segmentation of brain tumor lesions is important yet difficult due to the diverse shape and location of tumors. To achieve secure and private model training, this work proposes a federated learning framework over a blockchain infrastructure. Only the encrypted model parameters are shared on a permissioned blockchain, enabling decentralized learning without compromising raw data privacy. Experimental findings indicate that our approach enhances segmentation performance considerably, thereby facilitating medical image analysis and treatment programming [9].

Purohit et al. (2025),With the need for smart devices like smartwatches, personal healthcare data is only secured. In this work, we propose a framework that combines deep learning and federated learning with IPFS (InterPlanetary File System) and blockchain to anonymize and secure the storage of healthcare data. Federated learning allows you to train models without sharing raw data, and blockchain gives you transparent, immutable data access. Based on the results obtained, this system does not require any additional data to be released and delivers only the final learning model, with the advantage that it achieves an accuracy of 84.59% on CIFAR-10 and can be used for health care data privacy, ensuring secured records for sensitive data [10].

Khan et al. (2025),The digitization of healthcare has resulted in an enormous amount of electronic medical records (EMRs), presenting a great opportunity for medical research but also raising issues of privacy and security. We propose a framework for federated learning integrated with the blockchain to enable different institutions to collaboratively train machine learning models while keeping raw data localized. Using cryptography, blockchain allows for integrity and immutability of data, smart contracts facilitate trust, and both facilitate secure collaboration in medical research without compromising patient privacy. Experimental validation demonstrates its effectiveness and capacity to disrupt health care innovation [11].

Hai et al. (2024),In the era of Healthcare 5.0, which is characterized by the broad implementation of Internet of Things (IoT) and connected medical technologies, protecting the privacy of the patient is of vital importance. This research proposes a blockchain-system-federated learning and deep extreme machine learning based system in an effective and secure manner. This framework is implemented with various machine learning algorithms such as LDA, Decision Tree and AdaBoost to predict the disease with the usage of intrusion detection framework to avoid their security threats. Results show high accuracy and strong privacy preservation, which makes it an appropriate solution for secure and privacy-preserved health care systems [12].

Almalki et al. (2024),As more devices are connected to the Internet of Medical Things (IoMT), there is a growing concern about device and data security. In this paper, we propose the integration of blockchain and intrusion detection management (IDM) techniques to improve secure healthcare monitoring in federated learning. Designing and implementing an adaptive pathogenicity prediction model based ona CNNs trained exclusively using NCBIs dataset with an accuracy %- of 93.89% is achieved USD 43.13% in detecting the intrusion with this model. It can easily be the best way to increase the security and reliability for IoMT environments [13].

Myrzashova et al. (2024),Conventional approaches in ML risk the privacy of patient data, which makes federated learning a popular choice for collaboration. This paper presents a blockchain-based federated learning model to identify 15 lung diseases covered in the NIH Chest X-ray dataset (112,120 images). With 92.86% accuracy, the model shows 87% resilience against cyber attacks, meaning its prospects to contribute in care that is of secure scalable nature [14].

Khan et al. (2024),Conventional medical image diagnostics performed by humans and centralized systems are prone to errors and susceptible to attacks. This study introduces the FDEIoL (Healthcare Federated Ensemble Internet of Learning Cloud Doctor System) a federated ensemble learning technique for secure and accurate diagnosis within the scope of IoT and healthcare. Combining patient data at the edge addresses potential poisoning attacks while improving remote patient monitoring. The model achieves an accuracy of 99.24% on Chest X-rays and 99% on MRI brain tumor images, consistently outperforming centralized models in terms of diagnostic performance and robustness[15].

Kalinaki et al. (2024),We need a different solution, as traditional AI methods in healthcare are hampered by the centralization of data processing and privacy issues. Federated Learning (FL), a decentralized approach, supports secure machine learning, thus protecting the privacy of the IoHT devices. This paper examines FL deployment security issues and techniques to enhance privacy, like differential privacy and homomorphic encryption, which can provide guidance for secure FL for healthcare in future research [16].

Dhasaratha et al. (2024),IoMT help in COVID-19 patient monitoring, but data privacy is an adprivacy concern! To achieve data security, scalability, and efficiency, this study presents a blockchain-enabled reinforcement FL system. As no intermediate dependencies exist, the two can communicate securely to monitor the clinical

environment. We have combined all these results and have achieved a high reliability with performance improvement compared to the current methods [17].

Hamouda et al. (2023),With the roll-out of Industry 4.0/5.0, cyber-attacks and privacy violations. We propose PPSS, a blockchain-enabled FL framework for industrial IoT intrusion detection. To ensure security, verifiability, and transparency, it combines differentially private training with a Proof-of-Federated Deep-Learning (PoFDL) consensus protocol. Experiments on Edge-IIoT dataset show its efficiency against cyberattacks with zero-day malware under diverse distributions of data [18].

Kumar et al. (2025),Data fragmentation and poor predictive insights in conventional healthcare Here, we introduce an AI-based Smart Healthcare System that integrates Random Forest and K-means clustering for disease categorization (85–90% accuracy) and LSTM for sequential analysis. Data security and privacy law compliance (e.g. GDPR) with ETH blockchain Homomorphic encryption and differential privacy are some techniques that secure patient data while allowing for analytics [19].

Vyas et al. (2024),As IoT finds applications in healthcare, military, and defense systems, the security threats are also on the rise. This survey aims to give a thorough overview of the recent privacy-preserving federated learning (FL) frameworks focused on the intrusion detection systems (IDS) which combine various methods, such as homomorphic encryption, differential privacy, and secure multiparty computation. It also suggests future research directions in IoT security and emphasizes how FL solution can assist with both efficiently detecting cyber threats and preserving data privacy [20].

Markkandan et al. (2024),In this study, a CMD system based on privacy-preserving FL is proposed to improve the performance of real-time healthcare monitoring. FL also upholds data privacy by only sharing model parameters, whereas Partially Homomorphic Cryptosystem (PHC) and Residual Learning-based Deep Belief Network (RDBN) enhance not just classification accuracy, but security as well (451). This approach decreases overhead around 30%, while enhancing classification accuracy 10% on several datasets [21].

Malik et al. (2024),The swift acceptance of IoT technology in health care also brings security risks, given the sensitive nature of medical data. Data analytics and security is a huge challenge within the healthcare IoT domain, which attracts researchers and has been addressed in this study using blockchain and federated learning (FL) integration for Healthcare IoT systems. While FL leaves user data on users' devices, and allows for distributed, privacy-preserving machine learning, blockchain ensures all data and models remain in an immutable state. This paper mentions approaches for secure, shared health care analytics, and provides novel perspectives towards IoT Security and Privacy for compliance with Health Care needs [22].

Koutsoubis et al. (2024),Machine learning (ML) in medical imaging provides improved information for the diagnosis of diseases, however, the sensitive nature of medical images also implies privacy and security constraints. In this sense, Federated Learning (FL) solves this problem as it allows us to collaboratively train models while keeping data completely private without any direct data sharing between institutions. Nonetheless, FL is still an open problem, especially in terms of data heterogeneity and uncertainty estimation. This paper analyses FL, privacy techniques, and uncertainty quantification in medical imaging and highlights areas that demand more attention to improve the general framework [23].

Mahmud et al. (2024),Due to the centralized data collecting of conventional Intrusion Detection System (IDS)s, privacy problems arise. The proposed IDS in this study, an FL-based design for IoT networks, relies on Federated Averaging (FedAvg) to realize model weight aggregation from distributed devices. Compared to IDS models, the approach is scalable and privacy preserving with more than 90% accuracy rate for detection of DoS, DDoS and ransomware cyberattacks [24].

Shafik et al. (2024),This paper offers an extensive literature survey of Federated Learning (FL) security problems from various fields with specific emphasis on encryption, authentication and privacy-preserving methods. The paper critically assesses current FL frameworks and puts forward measures to improve data privacy and security especially in the context of healthcare. It is a valuable resource for practitioners, researchers, and policymakers as they navigate the growing importance of FL for data-driven decision-making [25].

Lazaros et al. (2024),Traditional centralized machine learning is subject to privacy, cost and compliance challenges. Federated Learning (FL) addresses these challenges by allowing distributed model training while preserving user data privacy and adherences to regulatory laws (e.g. GDPR) and reducing data transfer costs. This review provides a unique overview of FL's applications in IoT, including new insights toward applying FL framework for sensitive information during collaborative AI based implementation at industrial level [26].

Fouda et al. (2024),The Multitude of B5G (Beyond 5G) networks leads to enormous amounts of data arising, which necessitates the need for data analysis using privacy-preserving AI (Artificial Intelligence) models. We review data-driven privacy techniques such as differential privacy, homomorphic encryption, secure multiparty

computation, and FL, mapping them to emerging challenges in network security. It reviews the open research questions and presents solutions to thse challenges and opportunities for AI-enabled.

TABLE I. COMPARISON OF EXISTING RELATED WORK

Ref.	Highlight	Applications	Domains
[1] (2024)	Federated Learning Meets Blockchain in Decentralized Data Sharing	Healthcare	Federated Learning, Blockchain
[34] (2020)	Decentralized tourism destinations recommendation system	Tourism	Blockchain, data-sharing
[35] (2020)	Improving interorganizational information sharing for vendor managed inventory	Supply chain management	Blockchain, vendor-managed inventory
[36] (2019)	Building a secure biomedical data-sharing decentralized app	Biomedical research	Blockchain, data-sharing
[37] (2022)	Decentralized congestion control methods for vehicular communication	Vehicular networks	Blockchain, congestion control
[38] (2021)	Decentralized trusted data-sharing management on IoVEC networks	Internet of Vehicle Edge Computing	Blockchain, data-sharing
[39] (2020)	Decentralized data-sharing infrastructure for off-grid networking	Off-grid networking	Blockchain, data-sharing
[40] (2019)	Framework of data-sharing system with decentralized network	General data-sharing	Blockchain, data-sharing
[41] (2017)	P2P platform for decentralized	Logistics	Peer-to-peer, decentralized logistics
[42] (2022)	Decentralized network secured data-sharing	General data-sharing	Blockchain, data-sharing
[43] (2020)	Unlocking the potential of AI in assisted reproduction	Assisted reproduction	Blockchain, AI, data-sharing

III. METHODOLOGY

Combination of Fl and Blockchain for Decentralized Data Sharing

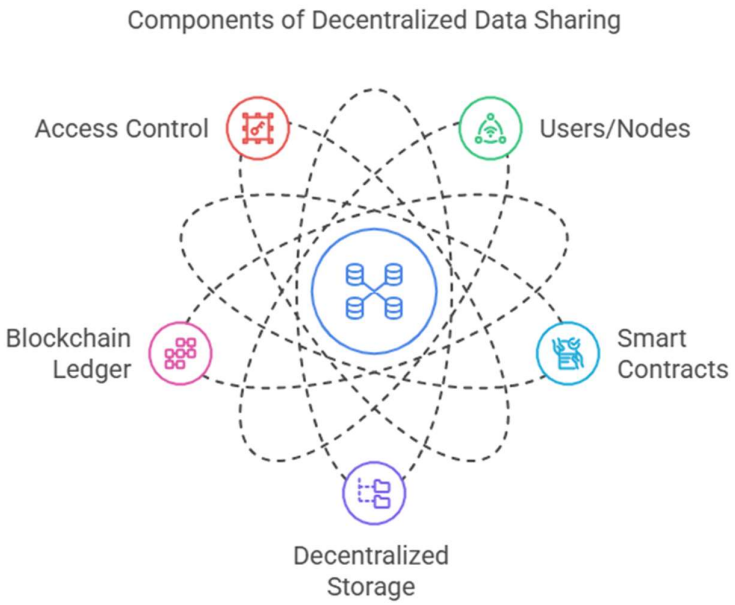

Figure 1. Decentralized data sharing.

In figure 1 decentralized data sharing includes access control, users/nodes, smart contract, decentralized storage and a blockchain ledger to ensure security, transparency and efficiency. Access control rules determine permissions while users/nodes share information and smart contracts handle conditional logic for safe transactions automatically. Decentralized storage ensures data availability without relying on a single authority while the blockchain ledger maintains an immutable record for trustworthiness and integrity. When combined, these components give a secure, scalable and transparent structure for the educational exchange of information of the decentralized kind across multiple platforms, including medical care, finance, and IoT networks.

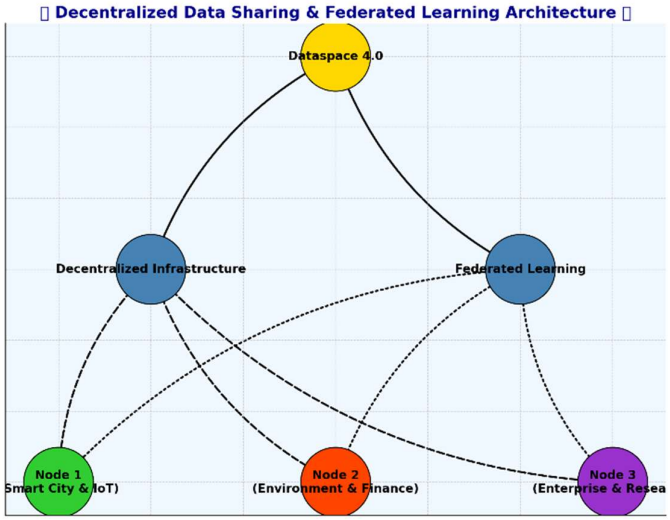

Figure 2. Decentralized Data Sharing and Federated Learning Architecture

The Decentralized Data Sharing and Federated Learning Architecture depicted in Figure 2 combines Dataspace 4.0, decentralization infrastructure and federated learning for secure, efficient and privacy-respecting data co-operation. The dispersed network comprising the Nodes representing Smart City & IoT, Environment & Finance and Enterprise & Research are interacting with each other while keeping raw data secured. While decentralized architectures promote trust in base systems, federated learning promotes training across nodes. Also known as Distributed Ledger technology, this paradigm offers superior data security, scalability, and interoperability making it suitable for healthcare, banking, and smart city applications.

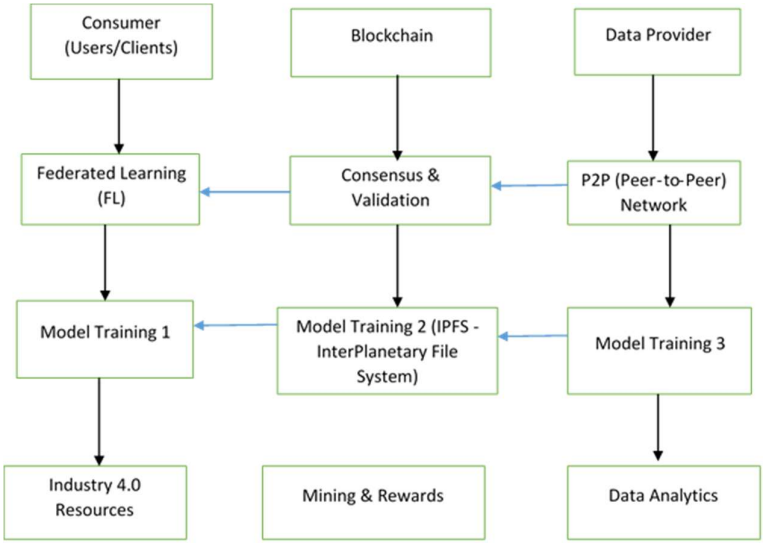

Figure 3. Combination of FL and blockchain for decentralized data sharing

TABLE II. COMPARING CENTRALIZED AND DECENTRALIZED DATA SHARING

Items	Centralization	Decentralization
Data control	Controlled by a single organization or authority	Distributed across multiple nodes
Security	Centralized control creates security risks	Distributed network of nodes improves resilience
Privacy	Centralized control creates privacy concerns	Encryption, and smart contracts enhance privacy
Interoperability	Limited interoperability	Improved interoperability with the use of decentralized standards and protocols
Transparency	Limited transparency and accountability	Tamper-proof and transparent record of data-sharing activities

TABLE III. DECENTRALIZED DATA SHARING WHEN BLOCKCHAIN MEETS FL

Aspect	FL	Blockchain	Combination
Enhanced Security and Privacy	FL enables data to be trained locally, reducing the risk of data exposure during transmission. However, FL does not inherently address data security during transmission.	Blockchain provides tamper-proof and encrypted data storage, ensuring the security and privacy of shared data.	FL with blockchain ensures end-to-end security, from data training to storage and sharing.
Data Integrity and Transparency	FL focuses on model updates and consensus, ensuring that the shared model is accurate and reliable.	Blockchain immutable and transparent data guarantees the integrity of shared data.	Combining FLs model updates with the blockchain data record, both models and data can be verified for authenticity.
Interoperability and Standardization	FL promotes collaboration across diverse devices and platforms for model training.	Blockchain establishes standardized protocols and smart contracts for data access.	Combining both ensures interoperable data-sharing mechanisms and a common data usage framework.
Decentralized Governance	FL allows data owners to retain control over their data and contribute to model training.	Blockchain decentralized consensus empowers participants to collectively agree on data-sharing terms.	Combining FL and blockchain extend this control to model updates and data access.
Resilience and Fault Tolerance	FL distributed nature ensures system resilience against participant failures.	Blockchain redundant data storage enhances resilience.	Combining both mitigates risks associated with individual participant failures.
Efficient Collaboration	FL facilitates collaborative model development.	Blockchain provides transparent and automated frameworks that streamline data-sharing processes.	FL and blockchain enhance efficient and trustworthy collaboration.
Data Monetization and Incentives	FL enables data owners to contribute to model training and earn incentives.	Blockchain tokenization and incentive mechanisms extend these rewards to data-sharing.	The combination encourages active data contribution.

TABLE IV. ADVANTAGES OF USING FL AND BLOCKCHAIN FOR DECENTRALIZED DATA SHARING

Feature	FL	FL with Blockchain
Data privacy	Data is kept private by each party, but may be vulnerable to attacks during transmission	Data is kept private by each party and is secured by the tamper-proof nature of the blockchain
Security	Requires trust between parties, and may be vulnerable to attacks or malicious behavior	Provides a secure and transparent record of the training process, making it more resistant to attacks or malicious behavior
Scalability	Can scale to large datasets, but may be limited by the communication bandwidth and computational resources of each party	Can scale to large datasets, but may be limited by the computational resources required to perform blockchain transactions
Cost	Lower cost compared to centralized training, but may still require significant resources and coordination between parties	Higher cost due to the computational resources required for blockchain transactions, but may provide increased security and transparency that justifies the cost
Accuracy	Can produce high accuracy if each party has representative data but may be affected by data heterogeneity or class imbalance	Can produce high accuracy if each party has representative data, and the blockchain can provide a mechanism for identifying and addressing data heterogeneity or class imbalance

TABLE V. BENEFITS OF DECENTRALIZED DATA SHARING IN DIFFERENT INDUSTRIES WITHIN THE CONTEXT OF INDUSTRY 4.0

Technology	Security	Privacy	Interoperability	Transparency	Resilience
FL	Encryption of data during transmission and storage	Data kept on local devices	Compatibility with different data formats	Limited transparency due to decentralized nature	Resilient to system failures
Blockchain	Immutable data storage	Decentralized control and verification	Ability to work across different systems	Publicly verifiable transactions	Resilient to tampering and attacks
Synergy of FL and blockchain	Multiple layers of encryption and verification	Data kept on local devices	Compatibility with different data formats	Publicly verifiable transactions	Resilient to tampering, attacks, and system failures

A. Result Analysis

Figure 4 involved in encryption and decryption as data size increases. Both encryption time (blue) and decryption time (red) show a linear growth pattern, with decryption consistently requiring slightly more time than encryption.

When the data size reaches approximately 50 KB, encryption takes around 9 ms, while decryption exceeds 10 ms. This underscores the resource-intensive nature of homomorphic encryption while demonstrating its

predictable scalability, making it a viable option for secure decentralized data sharing and federated learning in privacy-sensitive environments.

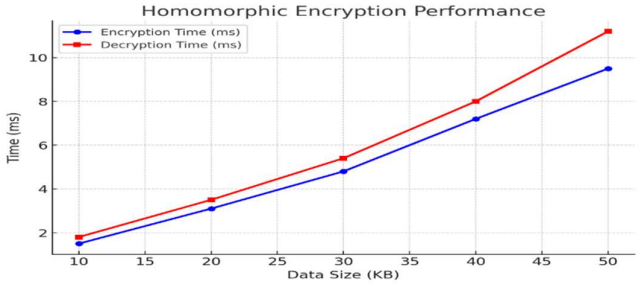

Figure 4. Homomorphic Encryption Performance

By integrating Federated Learning and Blockchain, healthcare systems can achieve a more secure, transparent, and efficient approach to medical data sharing. This innovative combination not only strengthens privacy protection but also fosters collaborative medical research, ultimately improving patient care and advancing healthcare analytics.

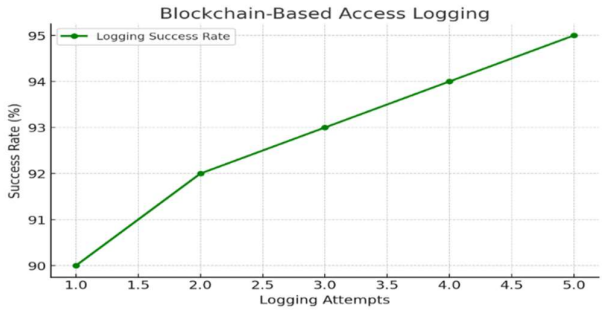

Figure 5. Blockchain-Based Access Logging

Figure 5 The Blockchain-Based Access Recording system demonstrates that the success rate of logging events improves with repeated attempts. Starting at 90% on the first attempt, the success rate gradually rises to 95% by the fifth attempt. This trend highlights blockchain's ability to ensure reliable and tamper-resistant logging, with enhanced consistency over successive operations. The results indicate improved data integrity and security, reinforcing blockchain's effectiveness as a robust tool for audit trails and access verification in decentralized data-sharing environments.

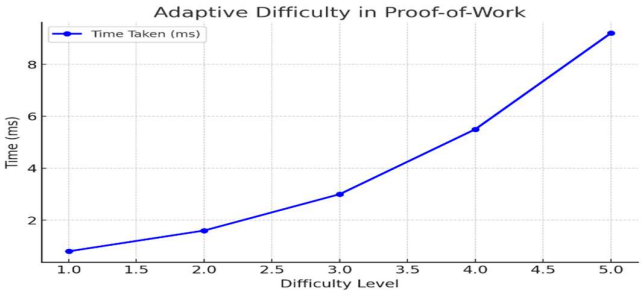

Figure 6. Adaptive Difficulty in Proof-of-Work

Proof-of-figure 6 Adaptive difficulty demonstrates how increasing difficulty levels impact the time required to solve cryptographic puzzles. As the difficulty progresses from level 1 to level 5, the computation time rises exponentially, reflecting the higher processing power needed for mining. This trend reinforces blockchain security by making it computationally expensive to reverse transactions. By deterring malicious activities, preventing spamming attacks, and regulating the block generation rate, adaptive difficulty serves as a fundamental mechanism for maintaining the stability and resilience of decentralized ledgers.

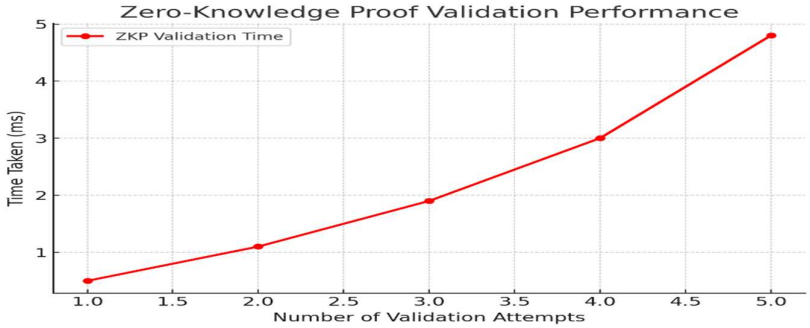

Figure 7. Zero-Knowledge Proof (ZKP) Validation Performance

Zero-Knowledge Proof (ZKP) validation exhibits strong performance, as illustrated in Figure 7, where validation time increases with the number of verification attempts. Initially, the validation time is minimal, but as the number of attempts grows, the time follows a non-linear curve, reaching approximately 5 ms by the fifth attempt. This underscores the computational cost of ZKP-based authentication, which enables identity verification without revealing sensitive information. The findings emphasize the significance of Location-ZKP in facilitating secure data sharing and authentication protocols, reinforcing privacy-preserving mechanisms in decentralized systems such as blockchain.

IV. Conclusion

Secure and efficient data exchange is crucial for protecting patient privacy and ensuring regulatory compliance in modern healthcare. Traditional centralized systems are prone to data breaches, security vulnerabilities, and compliance challenges, highlighting the need for decentralized alternatives. Federated Learning (FL) and Blockchain offer an innovative solution that enables privacy-preserving collaboration while maintaining data integrity and authenticity.

With FL, multiple healthcare organizations can collaboratively train machine learning models using local data without exposing raw patient information, significantly reducing security risks. However, FL alone lacks robust security protocols for data transfer, making it vulnerable to attacks. Blockchain, with its immutable and transparent ledger, strengthens security by ensuring tamper-proof data storage, decentralized identity management, and automated smart contracts.

The integration of Zero-Knowledge Proofs (ZKP) and Homomorphic Encryption further enhances privacy and enables secure computations. Additionally, Hyperledger Fabric facilitates secure transactions, while IPFS provides decentralized storage. The system leverages Proof of Stake (PoS) consensus, Multi-Factor Authentication (MFA), and AES-256 encryption to enhance security and reliability.This blockchain-based federated learning framework fosters trustless yet secure collaboration among data holders, enabling healthcare data sharing while preserving privacy. By mitigating cybersecurity risks, ensuring regulatory compliance, and promoting a decentralized, privacy-centric, and cost-effective healthcare ecosystem, this approach paves the way for a more secure and efficient future in medical data management.

References

[1] Stephanie, Veronika, Ibrahim Khalil, Mohammed Atiquzzaman, and Xun Yi. "Trustworthy privacy-preserving hierarchical ensemble and federated learning in healthcare 4.0 with blockchain." IEEE Transactions on Industrial Informatics 19, no. 7 (2022): 7936-7945.

[2] Alkhalifa, Amal K., Meshari H. Alanazi, Khalid Mahmood, Wafa Sulaiman Almukadi, Mohammed Al Qurashi, Asma Hassan Alshehri, Fuhid Alanazi, and Abdelmoneim Ali Mohamed. "Harnessing Privacy-Preserving Federated Learning With Blockchain For Secure Iomt Applications In Smart Healthcare Systems." Fractals 32, no. 09n10 (2024): 2540020.

[3] Ngoupayou Limbepe, Zounkaraneni, Keke Gai, and Jing Yu. "Blockchain-Based Privacy-Enhancing Federated Learning in Smart Healthcare: A Survey." Blockchains 3, no. 1 (2025): 1.

[4] Bezanjani, Behnam Rezaei, Seyyed Hamid Ghafouri, and Reza Gholamrezaei. "Fusion of machine learning and blockchain-based privacy-preserving approach for healthcare data in the Internet of Things." The Journal of Supercomputing 80, no. 17 (2024): 24975-25003.

[5] Guduri, Manisha, Chinmay Chakraborty, Uma Maheswari, and Martin Margala. "Blockchain-based federated learning technique for privacy preservation and security of smart electronic health records." IEEE Transactions on Consumer Electronics 70, no. 1 (2023): 2608-2617.

[6] Alzakari, Sarah A., Arindam Sarkar, Mohammad Zubair Khan, and Amel Ali Alhussan. "Converging Technologies for Health Prediction and Intrusion Detection in Internet of Healthcare Things with Matrix-Valued Neural Coordinated Federated Intelligence." IEEE Access (2024).
[7] Khan, Mohammad Faisal, and Mohammad AbaOud. "Blockchain-Integrated Security for real-time patient monitoring in the Internet of Medical Things using Federated Learning." IEEE Access (2023).
[8] Butt, Maryum, Noshina Tariq, Muhammad Ashraf, Hatoon S. Alsagri, Syed Atif Moqurrab, Haya Abdullah A. Alhakbani, and Yousef A. Alduraywish. "A Fog-Based Privacy-Preserving Federated Learning System for Smart Healthcare Applications." Electronics 12, no. 19 (2023): 4074.
[9] Kumar, Rajesh, Cobbinah M. Bernard, Aman Ullah, Riaz Ullah Khan, Jay Kumar, Delanyo KB Kulevome, Rao Yunbo, and Shaoning Zeng. "Privacy-preserving blockchain-based federated learning for brain tumor segmentation." Computers in Biology and Medicine (2024): 108646.
[10] Purohit, Ravindrakumar M., Jai Prakash Verma, Rachna Jain, and Ashish Kumar. "FedBlocks: federated learning and blockchainbased privacy-preserved pioneering framework for IoT healthcare using IPFS in web 3.0 era." Cluster Computing 28, no. 2 (2025): 1-15.
[11] Khan, Salabat, Mansoor Khan, Muhammad Asghar Khan, Lu Wang, and Kaishun Wu. "Advancing Medical Innovation through Blockchain-Secured Federated Learning for Smart Health." IEEE Journal of Biomedical and Health Informatics (2025).
[12] Hai, Tao, Arindam Sarkar, Muammer Aksoy, Rahul Karmakar, Sarbajit Manna, and Amrita Prasad. "Elevating security and disease forecasting in smart healthcare through artificial neural synchronized federated learning." Cluster Computing (2024): 1-26.
[13] Almalki, Jameel, Saeed M. Alshahrani, and Nayyar Ahmed Khan. "A comprehensive secure system enabling healthcare 5.0 using federated learning, intrusion detection and blockchain." PeerJ Computer Science 10 (2024): e1778.
[14] Myrzashova, Raushan, Saeed Hamood Alsamhi, Ammar Hawbani, Edward Curry, Mohsen Guizani, and Xi Wei. "Safeguarding Patient Data-Sharing: Blockchain-Enabled Federated Learning in Medical Diagnostics." IEEE Transactions on Sustainable Computing (2024).
[15] Khan, Rahim, Sher Taj, Xuefei Ma, Alam Noor, Haifeng Zhu, Javed Khan, Zahid Ullah Khan, and Sajid Ullah Khan. "Advanced federated ensemble internet of learning approach for cloud based medical healthcare monitoring system." Scientific Reports 14, no. 1 (2024): 26068.
[16] Kalinaki, Kassim, Adam A. Alli, Baguma Asuman, and Rufai Yusuf Zakari. "Secure federated learning in the Internet of Health Things for improved patient privacy and data security." In Federated Learning for Digital Healthcare Systems, pp. 387-408. Academic Press, 2024.
[17] Dhasaratha, Chandramohan, Mohammad Kamrul Hasan, Shayla Islam, Shailesh Khapre, Salwani Abdullah, Taher M. Ghazal, Ahmed Ibrahim Alzahrani, Nasser Alalwan, Nguyen Vo, and Md Akhtaruzzaman. "Data privacy model using blockchain reinforcement federated learning approach for scalable internet of medical things." CAAI Transactions on Intelligence Technology (2024).
[18] Hamouda, Djallel, Mohamed Amine Ferrag, Nadjette Benhamida, and Hamid Seridi. "PPSS: A privacy-preserving secure framework using blockchain-enabled federated deep learning for industrial IoTs." Pervasive and Mobile Computing 88 (2023): 101738.
[19] Kumar, Chanumolu Kiran, and G. Nagamani. "An Enhanced Model for Smart Healthcare by Integrating Hybrid ML, LSTM, and Blockchain." Ingénierie des Systèmes d'Information 30, no. 1 (2025).
[20] Vyas, Abhishek, Po-Ching Lin, Ren-Hung Hwang, and Meenakshi Tripathi. "Privacy-Preserving Federated Learning for Intrusion Detection in IoT Environments: A Survey." IEEE Access (2024).
[21] Markkandan, S., N. P. G. Bhavani, and Srigitha S. Nath. "A privacy-preserving expert system for collaborative medical diagnosis across multiple institutions using federated learning." Scientific Reports 14, no. 1 (2024): 22354.
[22] Malik, Rida, Hamza Razzaq, Chandradeep Bhatt, Keshav Kaushik, and Inam Ullah Khan. "Advancing Healthcare IoT: Blockchain and Federated Learning Integration for Enhanced Security and Insights." In 2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE), pp. 308-314. IEEE, 2024.
[23] Koutsoubis, Nikolas, Yasin Yilmaz, Ravi P. Ramachandran, Matthew Schabath, and Ghulam Rasool. "Privacy Preserving Federated Learning in Medical Imaging with Uncertainty Estimation." arXiv preprint arXiv:2406.12815 (2024).
[24] Mahmud, Syeda Aunanya, Nazmul Islam, Zahidul Islam, Ziaur Rahman, and Sk Tanzir Mehedi. "Privacy-Preserving Federated Learning-Based Intrusion Detection Technique for Cyber-Physical Systems." Mathematics 12, no. 20 (2024): 3194.
[25] Shafik, Wasswa, Kassim Kalinaki, Khairul Eahsun Fahim, and Mumin Adam. "Safeguarding Data Privacy and Security in Federated Learning Systems." In Federated Deep Learning for Healthcare, pp. 170-190. CRC Press.
[26] Lazaros, Konstantinos, Dimitrios E. Koumadorakis, Aristidis G. Vrahatis, and Sotiris Kotsiantis. "Federated Learning: Navigating the Landscape of Collaborative Intelligence." Electronics 13, no. 23 (2024): 4744.
[27] Fouda, Mostafa M., Zubair Md Fadlullah, Mohamed I. Ibrahem, and Nei Kato. "Privacy-Preserving Data-Driven Learning Models for Emerging Communication Networks: A Comprehensive Survey." IEEE Communications Surveys & Tutorials (2024).

[28] Gajndran, Sudhakaran, Revathi Muthusamy, Krithiga Ravi, Omkumar Chandraumakantham, and Suguna Marappan. "Elliptic Crypt With Secured Blockchain Assisted Federated Q-Learning Framework for Smart Healthcare." IEEE Access (2024).
[29] Senol, Nurettin Selcuk, Mohamed Baza, Amar Rasheed, and Maazen Alsabaan. "Privacy-Preserving Detection of Tampered Radio-Frequency Transmissions Utilizing Federated Learning in LoRa Networks." Sensors 24, no. 22 (2024): 7336.
[30] Gupta, Sharut, Sourav Kumar, Ken Chang, Charles Lu, Praveer Singh, and Jayashree Kalpathy-Cramer. "Collaborative privacy-preserving approaches for distributed deep learning using multi-institutional data." RadioGraphics 43, no. 4 (2023): e220107.
[31] Barnawi, Ahmed, Prateek Chhikara, Rajkumar Tekchandani, Neeraj Kumar, and Bander Alzahrani. "A Differentially Privacy Assisted Federated Learning Scheme to Preserve Data Privacy for IoMT Applications." IEEE Transactions on Network and Service Management (2024).
[32] Mahmood, Zeba, and Vacius Jusas. "Blockchain-enabled: Multi-layered security federated learning platform for preserving data privacy." Electronics 11, no. 10 (2022): 1624.
[33] Aljrees, Turki, Ankit Kumar, Kamred Udham Singh, and Teekam Singh. "Enhancing IoT Security through a Green and Sustainable Federated Learning Platform: Leveraging Efficient Encryption and the Quondam Signature Algorithm." Sensors 23, no. 19 (2023): 8090.
[34] 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.
[35] 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.
[36] 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.
[37] 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.
[38] 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.
[39] 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.
[40] 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.
[41] 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.
[42] 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.
[43] 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.