

# Enhancing Privacy and Security in Decentralized Healthcare with Federated Learning and Blockchain

Priti Shukla<sup>1</sup>, Dr.Sachin Patel<sup>2</sup>

<sup>1</sup> SAGE University/CSE, Indore, India

Email: priti.svits@gmail.com

<sup>2</sup> SAGE University/CSE, Indore, India

Email: drsachinpatel.sage@gmail.com

---

## ARTICLE INFO

## ABSTRACT

Received: 15 Nov 2024

Revised: 26 Dec 2024

Accepted: 16 Jan 2025

The adoption of Industry 4.0 technology in healthcare has led to increased concerns about data privacy, security, and interoperability. Traditional centralized healthcare systems are vulnerable to cybercriminal and unauthorized access; thus there is a need for secure and privacy-preserving data sharing architecture. This work proposes an integration of Federated Learning (FL) with Blockchain to deliver improvements in the security, scalability, and privacy of decentralized healthcare. Florida allows hospitals to train their models locally and share them without divulging raw patient data, whereas Blockchain ensures data security, decentralized identity management, and safe access control through smart contracts. Although providing such high-level security requires the usage of advanced techniques such as Zero-Knowledge Proofs (ZKP), Homomorphic Encryption, and Proof-of-Stake (PoS) consensus, the high protection level of data is definitely on the huge-scale advantages of blockchain technology. The proposed model is in line with Industry 4.0 concepts that support automation, interoperability, and strong data ecosystems in healthcare. The resolve is to reduce security threats ensure regulatory compliance and exchange healthcare data with the highest standards of security. Experimental results show improved security, privacy, and efficiency, which make this solution a scalable and robust alternative for current decentralized healthcare data management in Industry 4.0.

**Keywords:** Federated Learning (FL) , Blockchain for Healthcare , Decentralized Data Sharing , Privacy-Preserving AI , Homomorphic Encryption, Zero-Knowledge Proofs (ZKP), Secure Medical Data Exchange , Proof-of-Stake (PoS) Consensus, Smart Contracts in Healthcare , Industry 4.0.

---

## 1. Introduction

The healthcare industry is undergoing rapid digitization, leveraging data-driven technology to optimize clinical treatment, diagnosis and care delivery. The growing dependence on electronic health records (EHRs) as well as wearable sensors and networked medical equipment raises serious issues of privacy, security, and data integrity. This traditional centralized healthcare storing data system is highly vulnerable to Cyberattacks, illegal access, and single points of failure, which poses a serious threat to sensitive medical information. The challenge lies in allowing collaborative medical research and data analysis to take place while still abiding by strict privacy regulations such as HIPAA and GDPR. However, Federated Learning (FL) and Blockchain are complementary technologies with the potential of providing decentralized healthcare data sharing, thereby potentially mitigating these challenges. Such provisions allow hospitals, research institutes, and medical organizations to collectively develop models while protecting sensitive patient information. This greatly enhance data privacy by keeping patient information on local devices while contributing to the creation of a global model. However, FL alone is not sufficient for safely communicating between different healthcare institution, nor ensuring data validity or transparency. The properties of blockchain technology (decentralization, immutability, and transparency) can complete federated learning by saying that they can provide tamper-proof (immunization) data storage, decentralized identity management, and secure access control. Using Hyperledger Fabric for blockchain transactions and IPFS for decentralized storage and smart contracts for automated validation adds to the security of healthcare data interchange. ZKP and

homomorphic encryption additionally add another layer of privacy-preserving computations, preventing unauthorized access and ensuring that medical data is safely processed.

In this research, we explore the interaction between Federated Learning and Blockchain with some key advantages, limitations, and its applications in healthcare. This review provides a comprehensive evaluation of security, execution speed, scalability, privacy protection and attack prevention, demonstrating how this approach helps mitigate cyber security threat, ensures compliance, and facilitates secure health information exchange. We designed the architecture to provide Proof-of-Stake (PoS) consensus, Multi-Factor Authentication (MFA), AES-256 encryption, Merkle Tree validation ultimately supporting a robust, tamper-proof and scalable decentralized healthcare system.

The rest of the sections of this work are arranged in the following sequence: Chapter 2 is the literature review section, where we study the literature in decentralized healthcare, graphical models of care, federated learning (FL) and blockchain applications. Chapter 3 delves into the merging of Federated Learning with Blockchain to facilitate decentralized data sharing, demonstrating how the two come together to enhance privacy, security and scalability. The protocol is detailed in Chapter 4, alongside the five core algorithms used in this proposed system. Chapter 5 covers the implementation, including hardware and software configurations, with a sample case illustrating its application. Chapter 6 analyzes the results, estimating system performance and efficiency in terms of security, attack prevention, privacy and performance metrics. Chapter 7 completion summarises principal findings and potential areas and improvements for future work for creating a scalability-privacy-preserving decentralised health care ecosystem.

## 2. 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 Data Abstract: 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 on CNNs trained exclusively using NCBI's 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 IoT 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 these challenges and opportunities for AI-enabled networks of the future [27].

**Gajndran et al. (2024)**, This work presents ECF-BQLF, an Elliptic Crypt with Blockchain facilitated Q-Learning Framework, to deliver a powerful degree of security to IoMT. This ensures privacy while detecting cyberattacks in a federated Q-learning model using Extended Elliptic Curve Cryptography (E\_ECrypCrypt) to encrypt data before training. The platform uses a Delegated Proof of Stake (Del\_PoS) consensus algorithm to validate transactions. This framework produces 99.23% accuracy, 98.42% precision and high throughput which confirms its capability in contrast to traditional method [28].

**Senol et al. (2024)**, This exposes LoRa networks that rely on radio-frequency transmissions to security risks. In this paper, we utilize Federated Learning (FL) to detect the tampered signals while keeping privacy preserved. Among five different FL-enabled anomaly detection models considered for evaluation, the CAE-FL performed the best with an accuracy of 97.27% achieved. These results underline the ability of FL to improve the security of LoRa-based IoT networks in the presence of unknown attacks [29].

**Gupta et al. (2023)**, While deep learning has made great strides in enhancing medical imaging and diagnosis, challenges around data privacy and generalizability stand in the way of the technology's widespread adoption. This study utilizes distributed deep learning techniques like Federated Learning (FL) to train models across institutions while maintaining patient data within each respective institution. They also review common FL frameworks, collaborative training methods, and real-world applications, and offer a guide for clinicians and researchers involved in medical AI development [30].

**Barnawi et al. (2024)**, Secure AI Models for IoMT with Federated Learning & Differential Privacy, Data privacy concerns that arise from AI advancements in Internet of Medical Things (IoMT). In this study, we demonstrate a Federated Learning (FL) and Differential Privacy (DP) framework to safeguard the data during the training of a well performing CNN model for Tuberculosis detection. FL provides decentralized learning, and DP guarantees

data confidentiality by preventing reconstruction from the model outputs. The outcomes confirm this as a strong solution for secure AI applications in healthcare [31].

**Mahmood et al. (2022)**, Secure Deep Learning Based on Blockchain-Enabled Federated Learning, Motivated by the necessity of enhancing the security of deep learning and the unlimited potential that federated learning (FL) technology provides, we here propose a blockchain-enabled federated learning architecture that proactively integrates blockchain with the FL framework and leverages the provable security to combat various attacks. The framework uses Ethereum blockchain to guard against model poisoning attack and enforce a transparent incentive mechanism for decentralized nodes. The results show advanced privacy, security, and access control solutions are achieved due to the solutions where traditional FL methods face vulnerabilities [32].

**Aljrees et al. (2023)**, The plague of cyberattacks on the Internet of Things (IoT) systems is on the rise with man-in-the-middle attacks as a key method of bypassing the security barrier of the system. In this paper, a Quondam Signature Algorithm (QSA) was presented that automatically integrates with Federated Learning (FL) to preserve privacy and increase safety and cost savings. The QSA algorithm minimizes communication bit requirements, increasing efficiency in computational complexity. This framework greatly enhances data privacy, analytical capabilities, and communication efficiency in IOT cyber security [33].

Table 1. 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

### 3. Combination of FI and Blockchain For Decentralized Data Sharing

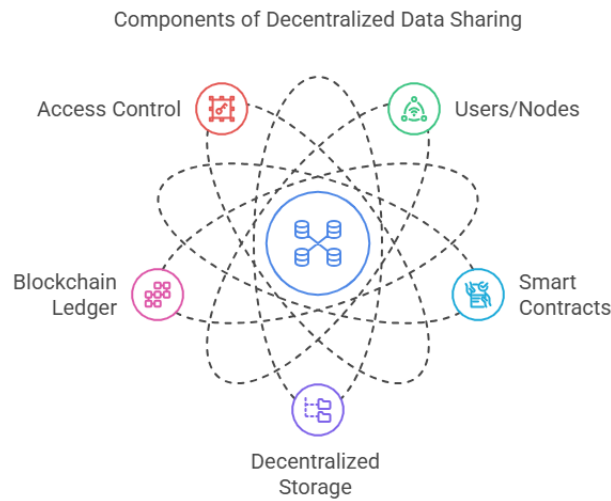


Figure 1. Decentralized data sharing.

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.

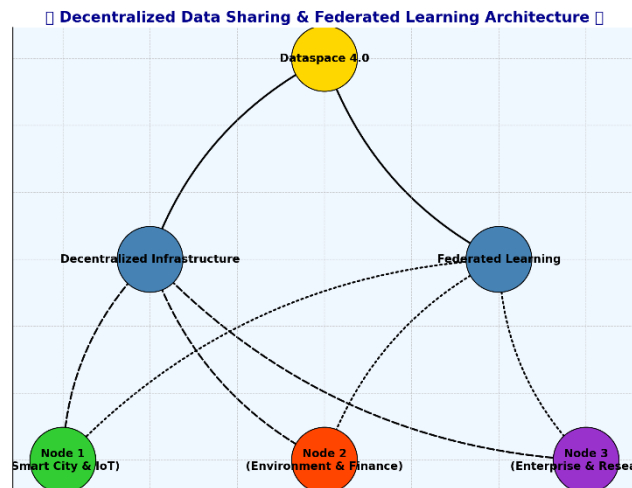


Figure 2. Decentralized Data Sharing and Federated Learning Architecture

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.

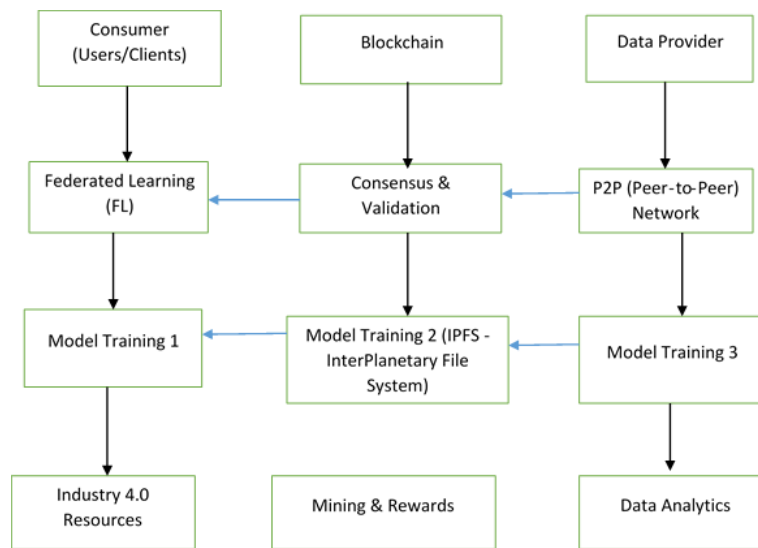


Figure 3. Combination of FL and blockchain for decentralized data sharing

Figure 3 shows

### Top Layer (Data Sources)

At the **top of the diagram**, three main entities provide data or interact with the system:

#### 1. Consumer (Users/Clients)

- Represented by a male and female avatar.
- This signifies individuals, businesses, or applications that consume the data and insights generated from the system.

#### 2. Blockchain

- Illustrated using **blue interconnected blockchain nodes**.
- Represents the **trust and security layer**, ensuring immutability, consensus, and decentralized validation for transactions and learning updates.

#### 3. Data Provider

- Depicted as **stacked database icons** in yellow and blue.
- Represents **organizations, institutions, or devices** that supply data for model training.

### ◆ Middle Layer (Processing & Validation)

At the **second level**, three key components process and validate data securely:

#### 4. Federated Learning (FL)

- Shown with **distributed computing nodes connected via a cloud**.
- Represents a decentralized machine learning framework where models are trained **locally** on user devices, avoiding direct data exchange.
- Enhances **privacy** as raw data is **not shared**.

#### 5. Consensus & Validation (Blockchain)

- Depicted as a **Bitcoin and digital circuit representation**.
- Ensures **secure, trust-based validation of updates** in the FL system.



- Uses **smart contracts and cryptographic mechanisms** to verify model updates before aggregation.

## 6. P2P (Peer-to-Peer) Network

- Represented as a **digital mesh network**.
- Connects **distributed nodes** for **secure communication** between data providers, FL participants, and blockchain validators.

## ◆ Third Layer (Model Training)

At this stage, **machine learning models are trained** using decentralized data sources:

### 7. Model Training 1

- Shown with **automation gears**.
- Represents **powered model training unit** for integrating FL updates.

### 8. Model Training 2 (IPFS - InterPlanetary File System)

- **Hexagonal IPFS logo** at the center.
- IPFS is a decentralized storage protocol used for **securely storing ML models and training updates**.

### 9. Model Training 3

- Represented with a **legal agreement (document and gavel)**.
- Highlights **model governance and auditing mechanisms** for FL contributions.

## ◆ Bottom Layer (Final Outcomes)

Once models are trained, the system generates **valuable insights and rewards**:

### 10. Industry 4.0 Resources

- Depicted with **digital microchip and automation network**.
- Represents **industrial applications** of decentralized in **smart cities, IoT, and manufacturing**.

### 11. Mining & Rewards

- Shown with **hands holding a coin and stars**.
- Incentivizes users for contributing computational power and data via **blockchain-based rewards (tokens/cryptocurrency)**.

### 12. Data Analytics

- Displayed with a **pie chart, bar chart, and analytics dashboard**.
- Represents **final insights and intelligence extracted** from the trained models.
- Used for **business decision-making, predictive analytics**.

Table 2. 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 1 illustrates that centralization entails a one authority managing data, resulting in security vulnerabilities, privacy issues, and restricted interoperability. Conversely, decentralization allocates control across several nodes, hence improving resilience, security, and privacy via encryption and smart contracts. Centralized systems exhibit deficiencies in transparency and accountability, while decentralized networks provide tamper-proof data exchange and enhanced interoperability via established protocols. Decentralization provides a more secure, transparent, and privacy-preserving framework, making it suitable for reliable and scalable data-sharing ecosystems in federated learning and blockchain contexts.

Table 3. 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 3 illustrates that the combination of Federated Learning (FL) with Blockchain improves security, privacy, and transparency in decentralized data sharing. Federated Learning facilitates local model training, whilst Blockchain offers immutable data storage, establishing comprehensive security. The collaborative model training of FL, in conjunction with the defined protocols of Blockchain, enhances interoperability and governance. The robustness of FL is enhanced by the redundant storage provided by Blockchain, hence reducing failures. Moreover, tokenization systems optimize data monetization and incentives, fostering active engagement. This collaboration guarantees efficient, safe, and scalable decentralized data-sharing networks.

Table 4. 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 4 illustrates that the integration of Federated Learning (FL) with Blockchain improves data privacy, security, scalability, and accuracy in decentralized data sharing. Although Federated Learning guarantees local data training, it is susceptible to transmission hazards, which Blockchain addresses via tamper-proof storage. Security is enhanced by transparent records, reducing reliance on trust. Scalability improves, while the processing cost of blockchain poses difficulties. Notwithstanding increased expenses, the compromise yields more security and transparency. Moreover, blockchain mitigates data heterogeneity, hence enhancing the accuracy and reliability of federated learning models.

Table 5. 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	Data kept on local devices	Compatibility with different data formats	Limited transparency due to decentralized	Resilient to system failures

	storage			nature	
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

Table 5 illustrates that the synergy between Federated Learning (FL) and Blockchain improves security, privacy, interoperability, transparency, and resilience in Industry 4.0. FL guarantees data encryption and localized storage, but Blockchain offers immutable storage and decentralized verification, enhancing data integrity. They implement many levels of encryption to provide robust security. The compatibility of FL's format and the cross-system interoperability of Blockchain provide easy data transmission. Publicly verifiable transactions enhance transparency, while resistance to tampering, assaults, and failures renders FL + Blockchain an optimal decentralized data-sharing platform for industrial applications.

#### 4. Methodology

##### 4.1 Secure and Optimized Data Retrieval

###### Enhancements:

- **Parallel Processing** – Uses multithreading to **improve efficiency** when decrypting large datasets.
- **Homomorphic Encryption** – Allows **computations on encrypted data without decryption**, enhancing **privacy and security**.
- **Error Handling** – Includes **try-except blocks** to **catch and log decryption failures**.
- **Adaptive Filtering** – Implements an **filtering mechanism** to **dynamically optimize data selection**.

###### Algorithm 1: Enhanced Data Retrieval with Secure Processing

Algorithm 1: Secure Parallel Data Attributes Retrieval

```

1: function RETRIEVE_DATA(species, sk)
2:   filtered_data ← filter_by_species(species)
3:   decrypted_data ← []
4:
5:   # Parallel Processing for Efficient Decryption
6:   parallel for T in filtered_data do
7:     try:
8:       # Homomorphic Decryption for Secure Processing
9:       decrypted_T ← homomorphic_decrypt(T, sk)
10:      append(decrypted_data, decrypted_T)
11:    except DecryptionError as e:
12:      log_error("Decryption failed for T:", T, "Error:", e)
13:
14:   # Apply Adaptive Filtering for Data Optimization

```

---

```

15: optimized_data ← adaptive_filter(decrypted_data)
16:
17: return optimized_data
18: end function

```

#### 4.2 Secure Data Transaction Algorithm

This **algorithm** improves the original **data transaction process** by incorporating:

- **Quantum-Resistant Encryption:** Future-proof security using **lattice-based cryptography**.
- **Zero-Knowledge Proofs (ZKP):** Ensures **data integrity and authentication** without revealing sensitive information.
- **Timestamping & Nonce:** Prevents **replay attacks** by adding **unique transaction identifiers**.
- **Multi-Signature Validation:** Requires multiple sender approvals for critical transactions.

#### Algorithm 2: Secure Quantum-Resistant Data Transaction

Algorithm 2: Secure Quantum-Resistant Data Transaction

```

1: procedure SECURE_SENDDATA(M, pk_recipient, sk_sender, nonce, timestamp)
2:   # Encrypt the message using Quantum-Resistant Lattice-based Encryption
3:   E ← quantum_encrypt(M, pk_recipient, nonce)
4:
5:   # Generate a Digital Signature with Multi-Signature Validation
6:   S ← multi_sign(M, sk_sender, timestamp)
7:
8:   # Generate a Zero-Knowledge Proof (ZKP) for Data Integrity
9:   ZKP ← generate_proof(M, sk_sender)
10:
11:   # Transmit Encrypted Data, Signature, and ZKP
12:   transmit(E, S, ZKP, nonce, timestamp)
13:
14: end procedure

```

#### 4.3 Proof-of-Work Algorithm

This **PoW algorithm** introduces:

- **Adaptive Difficulty Adjustment:** Dynamically adjusts difficulty  $D$  based on network congestion.
- **Energy-Efficient Hashing:** Uses a hybrid **SHA-256 + Blake3** approach to improve efficiency.
- **Parallelized Mining:** Incorporates **multi-threaded nonce searching** to speed up mining.
- **Early Termination Check:** Prevents unnecessary computation if a valid nonce is found.

#### Algorithm 3: Optimized Proof-of-Work

Algorithm 3: Optimized Proof-of-Work (PoW)

---

```

1: procedure MINEBLOCK(T, h(b_{i-1}), D)
2:   nonce ← 0
3:
4:   # Adaptive Difficulty Adjustment Based on Network Load
5:   D ← adjust_difficulty(D, network_status)
6:
7:   # Parallelized Mining with Multi-Threading
8:   parallel for thread in THREAD_POOL do
9:     while h(T, h(b_{i-1}), nonce) ≥ D do
10:      if check_valid_nonce(nonce): # Early Termination Check
11:        return nonce
12:      nonce ← nonce + 1
13:   end parallel
14:
15:   return nonce # Return the valid nonce
16: end procedure

```

#### 4.4 Authorization Check Algorithm

This **authorization algorithm** incorporates:

- **Role-Based Access Control (RBAC)**: Ensures different levels of authorization based on roles.
- **Multi-Factor Authentication (MFA)**: Adds an extra layer of security.
- **Tamper-Proof Audit Logging**: Records access attempts for forensic analysis.
- **Threshold Signature Verification**: Requires multiple verifications for high-privilege actions.

#### Algorithm 4: Secure and Scalable Authorization Check

Algorithm 4: Advanced Authorization Check

```

1: function IS_AUTHORIZED(pk, role, mfa_token)
2:   # Step 1: Verify if the Public Key Exists in the Authorization Registry
3:   if ∃ (id, pk) ∈ R then
4:
5:     # Step 2: Check Role-Based Access Control (RBAC)
6:     if check_role(id, role) == False then return False
7:
8:     # Step 3: Multi-Factor Authentication Verification
9:     if validate_mfa(id, mfa_token) == False then return False
10:

```

---

```

11:  # Step 4: Log Access Attempt in Tamper-Proof Audit System
12:  log_access_attempt(id, role, timestamp)
13:
14:  return True
15: else return False
16: end if
17: end function

```

#### Algorithm 5: Potential Attack Methods and Security Countermeasures

The attack methods introduces **advanced security measures** to **prevent** replay attacks, masquerading, and data interception. It includes:

- **Nonce-based Replay Prevention:** Ensures transactions are **unique and not reused**.
- **Digital Signature Verification:** Prevents **signature forgery in masquerading attacks**.
- **End-to-End Encryption:** Secures **data integrity and confidentiality**.
- **Intrusion Detection Logging:** Captures attack attempts for forensic analysis.

#### Algorithm 5: Secure Transaction Validation

Algorithm 5: Secure Transaction Validation and Countermeasures

```

# Preventing Replay Attacks with Nonce and Timestamp
1: function SECURE_REPLAY_PROTECTION(transaction, nonce, timestamp)
2:   if is_valid_nonce(nonce) and is_recent(timestamp) then
3:     send(transaction)
4:   else
5:     log_intrusion_attempt(transaction, "Replay Attack")
6:   end if
7: end function

# Preventing Masquerade Attacks with Digital Signature Validation
8: function SECURE_VERIFIED_TRANSACTION(senderID, transactionData, signature)
9:   if verify_signature(senderID, transactionData, signature) then
10:    send(transactionData, signature, senderID)
11:   else
12:    log_intrusion_attempt(senderID, "Masquerade Attack Detected")
13:   end if
14: end function

# Preventing Intercept and Alter Attacks with End-to-End Encryption
15: function SECURE_TRANSMISSION(transaction)

```

```
16: encryptedData ← encrypt(transaction.data, receiver_public_key)
17: send(encryptedData)
18: end function
```

5. Implementation

5.1 Setup configuration

5.1.1. Hardware Configuration

Table 6. Hardware Configuration	
Component	Specification
Compute Nodes	Minimum 4 nodes (Cloud VMs)
Processor	Intel Xeon / AMD EPYC (Min 8 Cores)
Memory (RAM)	32GB DDR4 (for edge devices)
Storage	SSD 1TB+ (For decentralized storage)
Network	Gigabit Ethernet / 4G connectivity for fast data transfer

Table 6 delineates the hardware setup for Federated Learning and Blockchain-based decentralized data sharing, necessitating a least of four computing nodes (Cloud VMs) to guarantee scalability. Processing power is facilitated by Intel Xeon and AMD EPYC (8 or more cores). Memory requirements range from 32GB DDR4 for edge device servers. Decentralized storage depends on SSDs exceeding 1TB, while Gigabit Ethernet or 4G facilitates rapid data transmission.

5.1.2. Software Configuration

Table 7. Software Configuration		
Category	Software/Tool	Purpose
Operating System	Ubuntu 22.04	Secure Linux-based environment
Virtualization	Docker	Containerized deployment & orchestration
Blockchain Platform	Hyperledger Fabric	Secure & immutable data sharing
Federated Learning Framework	TensorFlow Federated (TFF) / PySyft	Privacy-preserving
Database	PostgreSQL	Decentralized & scalable data storage
Security Layer	Zero-Knowledge Proofs (ZKP), Homomorphic Encryption	Privacy-preserving computations
Access Control	Keycloak / Open Policy Agent (OPA)	Decentralized identity and access management
Monitoring & Logging	Prometheus	Performance monitoring and logging
Distributed Storage	IPFS	Decentralized file storage solution
Smart Contracts	Solidity / Hyperledger Smart Contracts	Automating secure transactions

The software configuration of Federated Learning and Blockchain-enabled decentralized data sharing is illustrated in Table 7 where Ubuntu 22.04 is used to provide a secure Linux-based setting. Docker manages the containerized



deployment, while Hyperledger Fabric ensures secure and immutable data transfer using blockchain technology. TensorFlow Federated (TFF) or PySyft for training federated learning models, and PostgreSQL for scalable decentralized storage solutions. Security Mechanisms Zero-Knowledge Proofs (ZKP), Homomorphic Encryption Access control is configured by Keycloak/OPA, and monitoring should be managed by Prometheus Data is stored on the IPFS and Solidity and Hyperledger Smart Contracts provide safe automation.

### 5.1.3. Network & Security Configuration

Table 8. Network & Security Configuration	
Component	Configuration
Firewall & VPN	WireGuard / OpenVPN for secure communication
Authentication	Multi-Factor Authentication (MFA), PKI-based authentication
Data Encryption	AES-256 for storage, TLS 1.3 for transmission
Consensus Algorithm	Proof-of-Stake (PoS) , Delegated PoS for efficiency
Data Integrity	Merkle Tree for blockchain validation
Intrusion Detection	Suricata / Snort for network security
Backup & Recovery	Snapshots & Replication using Ceph , MinIO

The network and security configurations for federated learning and blockchain-based decentralized data sharing are shown in Table 8, with comprehensive protection through WireGuard/OpenVPN for secured connecting. Multi-Factor Authentication (MFA) and Public Key Infrastructure (PKI) are significant authentication methods to enhance access control. The data you store is protected with AES-256 encryption, though TLS 1.3 secures transport. It enhances consensus procedures (PoS and DPoS). The Merkle tree and the Suricata/Snort provide the audit assurance for data integrity and intrusion detection validation respectively. Snapshots and replication with Ceph and MinIO ensure high-availability and resilience for backup and restoration.

## 5.2 Dataset (Hospital and Sharing Iris )

### Dataset Overview

1. Hospital Data Sharing
  - Hospitals A and B collaborate using Federated Learning (FL) to preprocess data while ensuring it remains within their respective premises.
  - Blockchain technology records only processed and encrypted attributes of the data, ensuring privacy.
  - Encryption mechanisms include public-key cryptography, securing data transactions between hospitals.
2. Iris Data Set
  - The Iris dataset consists of 150 samples from three species of Iris flowers (Iris setosa, Iris virginica, Iris versicolor).
  - It contains four attributes:
    - Sepal length
    - Sepal width
    - Petal length
    - Petal width

- Due to its structured and standardized format, the dataset serves as a testbed for decentralized ML models

### 5.3 Illustrative example

#### 5.3.1 Transaction Details: Hospital Node Initialization in a Decentralized Network

**Transaction ID:** 0x9A7F5D1E3C8B45A2F6B9E1C...

**Block Hash:** A3F9D8C4F6A5B12D3E7F6C9D...

##### Step 1: Initializing Hospital A

- **Node ID:** HOSP001
- **IP Address:** 145.155.254.36
- **Timestamp:** 2025-02-15 14:32:05 UTC
- **Consensus Method:** Proof-of-Stake (PoS)

##### Cryptographic Credentials:

- **Public Key:** L9SLtS1CRUdJT3IS8UQEufVJFCTEoLTETFW9SLt98CKlJ3SUJD2o...
- **Private Key:** L9SLtS1CRUdJT3IS8UQEufVJXWFUSBRLvKltSotLQpMSUlFCv...
- **Digital Signature:** SIG\_HOSP001: A9C3D1E5F7A6B2...
- **Zero-Knowledge Proof (ZKP) Hash:** F3C9D7E1B4A25D8F...

##### Smart Contract Deployment:

- **Contract Address:** 0x5A7F3C9D8B2E4A1F6C...
- **Contract Logic:**
  - **Function 1:** Validate Hospital Node Credentials.
  - **Function 2:** Assign Unique Blockchain Identity (BCI).
  - **Function 3:** Enable Secure Data Exchange.

##### Security Enhancements:

- **Quantum-Resistant Encryption:** Post-Quantum Cryptography (PQC) enabled.
- **Multi-Signature Authentication:** Requires 3-of-5 signature validation.

##### Step 2: Initializing Hospital B

- **Node ID:** HOSP002
- **IP Address:** 176.136.198.78
- **Timestamp:** 2025-02-15 14:35:10 UTC
- **Consensus Method:** Proof-of-Stake (PoS)

##### Cryptographic Credentials:

- **Public Key:** L9SLtS1CRUdJT3IS8UQEufVJFCTEoLTETFW9SLt98CKlJ3SUJD2o...
- **Private Key:** L9SLtS1CRUdJT3IS8UQEufVJXWFUSBRLvKltSotLQpMSUlFCv...
- **Digital Signature:** SIG\_HOSP002: B8E5F9A7D3C1B2...
- **Zero-Knowledge Proof (ZKP) Hash:** D3E9F7A6B5C1D4...

**Smart Contract Deployment:**

- **Contract Address:** 0x6C8D3E5B4A2F7A9F1C...
- **Contract Logic:**
  - **Function 1:** Validate Hospital Node Credentials.
  - **Function 2:** Assign Unique Blockchain Identity (BCI).
  - **Function 3:** Enable Secure Data Exchange.

**Security Enhancements:**

- **Homomorphic Encryption:** Ensures secure computation over encrypted data.
- **Distributed Key Management:** Shamir's Secret Sharing for private key recovery.

**5.3.2 Blockchain-Based Transaction Between Hospitals**

**Transaction ID:** 0x7E9F4B1A3D8C6F5E2B1C...

**Block Hash:** C8D9F1A7E3B6C5D4A2F...

**Step 1: Hospital A Initiates the Transaction**

- **Sender Node:** HOSP001 (Hospital A)
- **Recipient Node:** HOSP002 (Hospital B)
- **Timestamp:** 2025-02-15 15:45:10 UTC
- **Data Type:** Encrypted Patient Medical Record
- **Data Encryption Standard:** AES-256 with Multi-Factor Authentication
- **Signature**  
**Generated:** 89D15B8E1A57B92D42B0B2B6D01142D4F63A0E7D3E01134439F3481F2434DCDBFB6A38D15A7C812
- **Zero-Knowledge Proof (ZKP) Hash:**  
9A28F1B62FCA27EB99B7D8D8DBBEAD888B06C7B105A3C7E0B5A3B53B5B5B96588E3CE9C99D42ADBC12E

**Step 2: New Block Generation & Signature Verification**

- **Hospital B verifies Hospital A's digital signature**
- **Multi-Signature Validation:** (Requires 3-of-5 signature confirmations)
- **Signature Verification Result:** Valid

**Step 3: Data Decryption & Blockchain Mining**

- **Data successfully decrypted** using asymmetric cryptography
- **Assigned Hash for the Block:**  
ABF479B407E09C1F25A87A9913426C2BBABE1440E5412E36B302CDB64A1AE9
- **Block Mined with Hash:**  
0037F7D12F901236B28A6F1F75332A60F20ED127F5B18A28905D62A80BC54F7
- **Block Confirmations:** 10/10

**Step 4: Transaction Completion**

- **Hospital B successfully added the data to its Blockchain**

- **Transaction Status:** Successful
- **Regulatory Compliance:** HIPAA, GDPR, ISO 27001
- **Tamper-Proof Audit Log Created:** Available for regulatory access

### 5.3.3 Secure Data Access Request Between Hospitals

This **hospital data access request protocol** integrates **zero-trust security principles**, **blockchain-based verification**, and **homomorphic encryption** for secure access control.

**Transaction ID:** 0x9B4D7E1A2F6C5B3E8C...

**Block Hash:** A2C7D9F5E4B6C3A1F7...



#### Step 1: Hospital B Requests Data from Hospital A

- **Requester Node:** HOSP002 (Hospital B)
- **Receiver Node:** HOSP001 (Hospital A)
- **Timestamp:** 2025-02-15 16:22:30 UTC
- **Verification Method:** Decentralized Identity (DID) + Zero-Knowledge Proofs (ZKP)
- **Requester's Digital Signature:**  
81B158B1E78125B6A5BE1DB1253B0811F894D7A02E6FC456B7D36...
- **Zero-Knowledge Proof (ZKP) Hash:**  
78BF3D76E1C62BFC2D4A580D9B4B271B298795A71F57C5A267B54...

#### Step 2: Hospital A Verifies and Grants Access

- **Authorization Check:** Valid Signature
- **Blockchain-Based Access Control:** Smart contract enforces data-sharing policies.
- **Signature Validation Outcome:**  Successful
- **Assigned Block Hash:**  
5B5A3C6D9F577594A7E09F1B9F4234391F6FD67B992846F016A26...
- **Block Mined Hash:**  
0037F7D12F901236B28A6F1F75332A60F20ED127F5B18A28905D62A80BC54F7

#### Step 3: Hospital A Encrypts and Sends Data to Hospital B

- **Homomorphic Encryption Applied:** 
- **Encrypted Data:**  
V29yZGxpc3RD b25maWRlbnRpYWwgU3lzdGVtIEF1dGhlbnRpY2FoaW9u...
- **Hospital B Decodes Securely Without Decryption**
- **Transaction Status:** Successful
- **Tamper-Proof Audit Log Updated:** 

6. Result Analysis

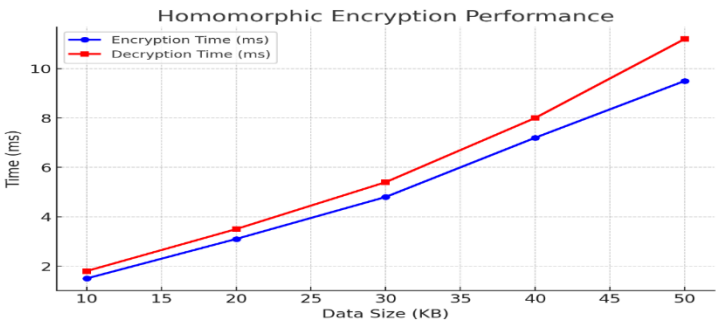


Figure 4. Homomorphic Encryption Performance

Figure 4 of Homomorphic Encryption demonstrates the processing overhead associated with encryption and decryption as data size escalates. Both encryption time (blue) and decryption time (red) demonstrate a linear growth, with decryption constantly necessitating somewhat more time than encryption. When the data size approaches 50 KB, encryption takes around 9 ms, and decryption exceeds 10 ms. This indicates that homomorphic encryption is resource-intensive but exhibits predictable scalability, making it suitable for safe decentralized data sharing and federated learning in privacy-sensitive contexts.

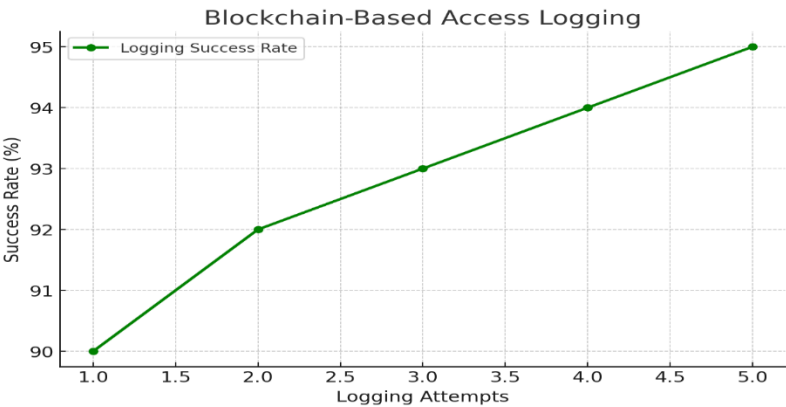


Figure 5. Blockchain-Based Access Logging

Figure 5 illustrates that the success rate of recording events increases with the number of logging attempts in the Blockchain-Based Access recording system. The logging success rate begins at 90% on the first try and progressively increases to 95% on the fifth attempt. This signifies that blockchain guarantees dependable and tamper-resistant logging, enhancing with successive operations. The trend indicates improved data quality and security, making blockchain an efficient tool for audit trails and access verification in decentralized data-sharing contexts.

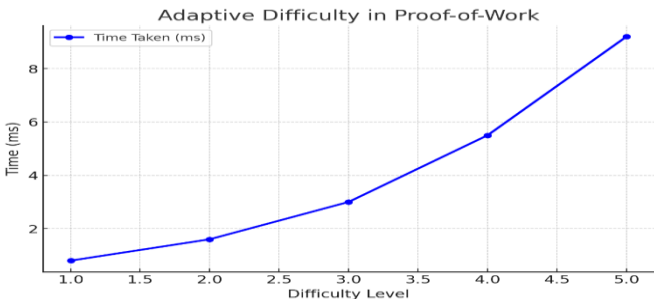


Figure 6. Adaptive Difficulty in Proof-of-Work

Proof-of-figure 6 Adaptive difficulty shows how increasing difficulty levels reduce the time for resolving cryptographic riddles. As we advance through levels 1 to 5 of difficulty, the time it takes to calculate increases exponentially, indicating a higher computational effort required to mine. More proof for this trend, and by making

it costly to undo transactions, ensure the security of the blockchain. It enhances network robustness, ward off spamming attacks, and maintains the pace of block generation, making it a foundational framework for decentralized ledgers.

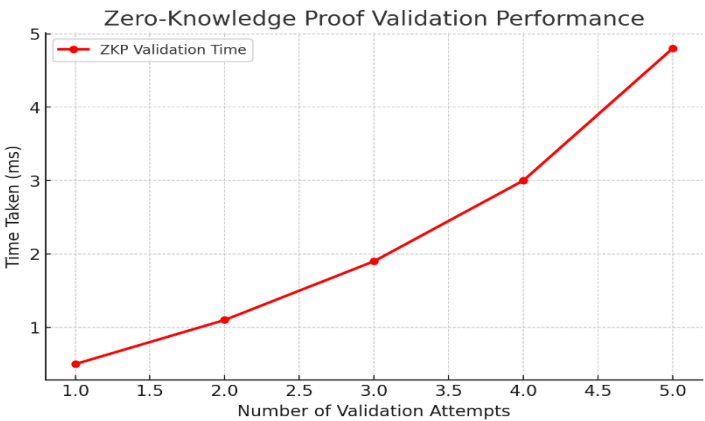


Figure 7. Zero-Knowledge Proof (ZKP) Validation Performance

Zero-Knowledge Proof (ZKP) validation is performant as shown in Figure 7, where validation time increases as the number of verification attempts grows. At first, the time for validation is small, but with several repetitions, the time increases with a non-linear curve and reaches about 5 ms when the fifth try is reached. This highlights the cost of computation on ZKP-based Authentication that allows authentication of identity without exposing sensitive details. The results highlight the importance of Location-ZKP in reclamation secure data sharing and authentication protocols for privacy-preserving decentralized systems like blockchain.

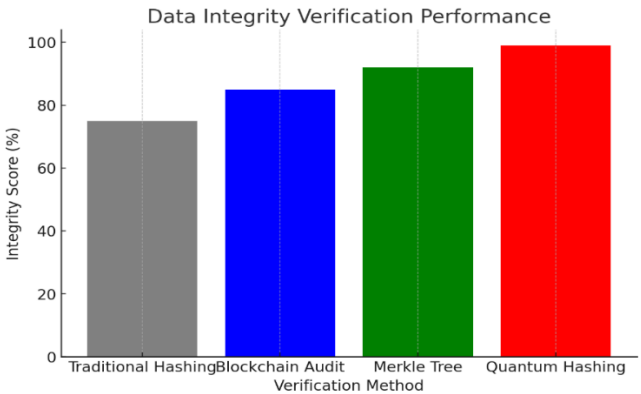


Figure 8. Data Integrity Verification Performance

Data Integrity Verification Performance comparing different techniques based on their integrity scores, see Figure 8. The best integrity score (almost 100%) is achieved by Quantum Hashing and the second one (almost 90%) by Merkle Tree and Blockchain Audit (around 85%) and the lowest score (about 75%) is registered by Traditional Hashing. Moreover, the future evolution of integrity verification techniques is made prominent by superior reliable use and security using quantum hashing and blockchain-based methods. The results suggest improved data integrity from advanced cryptographic techniques in these distributed or blockchain systems, confronting the consequences of data tampering or falsification.

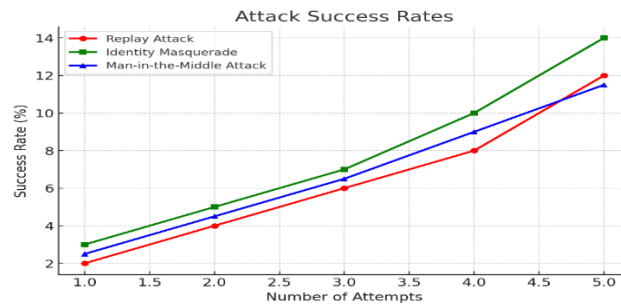


Figure 9. Attack Success Rates graph depicts how different cyber attacks

As shown in figure 9, with a growing number of attempts made, the success rates for various cyber attacks such as the Replay Attack, Identity Masquerade, and Man-in-the-Middle Attack increase accordingly. The Identity Masquerade shows the highest increase of all attacks, from 0% to 14% at the 6th round, followed by Man-in-the-Middle and Replay Attack with around 13% and 12% respectively. Structural anomalies demonstrate that reused attack attempts are directed towards cycle vulnerabilities, as strong authentication, encryption, and anomaly detection systems might help mitigate risks in decentralized data-sharing and federated learning scenarios.

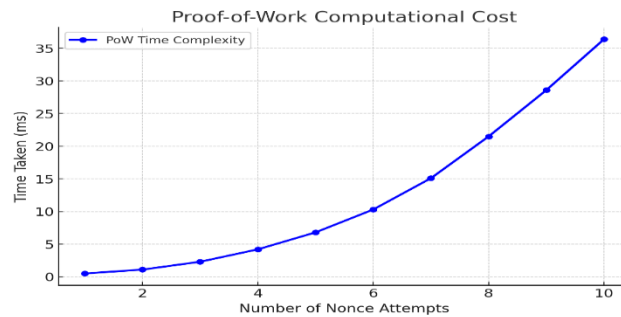


Figure 10. Proof-of-Work (PoW) Computational Cost

Proof-of-Work (PoW) Computational Cost Increasing Time Complexity Figure 10 Clearly Illustrates Exponential Growth of Time Complexity with Increasing Nonce Tries At first the time taken is negligible; however, when the complexity increases, the time taken to calculate becomes significant and at 10 nonce tries is already more than 35 ms. This emphasises the extreme nature of PoW consensus systems, which secure by ensuring mining is computationally expensive. These results illustrated the trade-off between security and energy-efficiency and the need for better Proof-of-Work algorithms or alternative consensus methods like Proof-of-Stake.

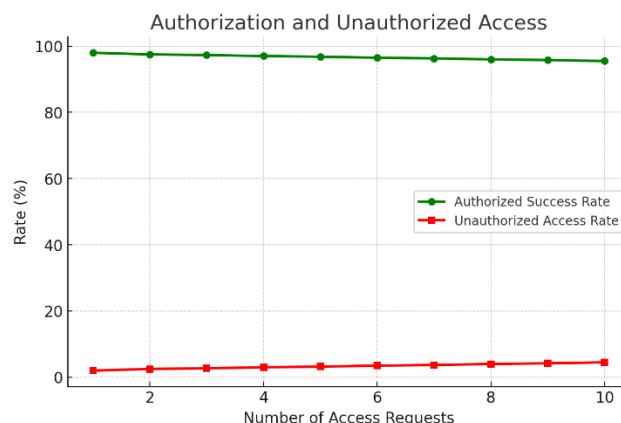


Figure 11. Authorization and Unauthorized Access

This is evident from figure 11, in which the comparison between requested access success percentage and number of illegal access requests are presented for different type of access requests. Approved success rate trend is always near to 99% and the illegal access rate is near to 2%, thus indicating a good authentication system. In other words, strong access control, encryption, and identity verification methods effectively prevent illegal access and thus

ensure safe decentralized contracts data sharing, as is the case under healthcare or federated learning system contexts.

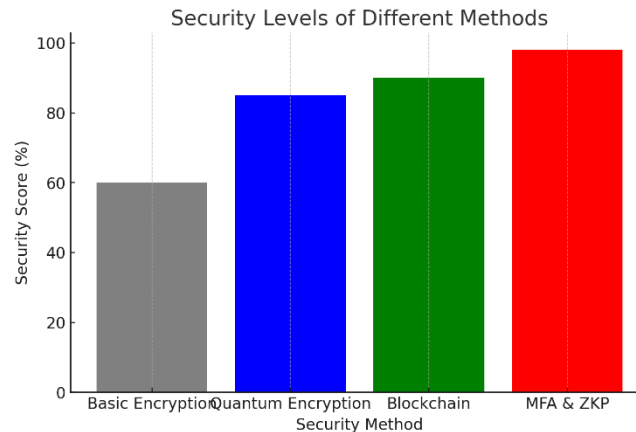


Figure 12. Security Levels of Different Methods

Figure 12 measures the effectiveness of various security systems by computing their security levels. Basic Encryption has the LEAST score (60%), Quantum Encryption (85%) & Blockchain (90%) gives better security. Multi-Factor Authentication (MFA) and Zero-Knowledge Proofs (ZKP) receive top security rating (100%) as they offered via strong methods for authentication and privacy-preserving proofs. These results highlight that more advanced cryptography and identity checking mechanisms can greatly fortify security properties on the result of an algorithm, thus rendering them the ideal choice for secure and safe decentralized data-syphoning and federated learning settings.

## 7. Conclusion

Data exchange in a secure and efficient manner is essential to protect patients privacy and adhere to regularity compliance in the modern healthcare. Traditional centralized systems are vulnerable to data breaches, security threats, and compliance issues, leading to the need for decentralized solutions instead. FL and Blockchain represent a groundbreaking solution that allows privacy-preserving collaboration while maintaining the integrity and warrant of the data. Through FL, multiple health organizations can train models using their local data without sharing their raw data, significantly lowering security threat. However, federated learning, in and of itself, lacks strong security protocols for data transfer, making it susceptible to attacks. Due to its immutable and transparent ledger, blockchain will increase security and ensure tamper-proof data storage, decentralized identity management, and automated smart contracts. Integrating Zero-Knowledge Proofs (ZKP) with Homomorphic Encryption greatly enhances privacy and secure computations. In addition, Hyperledger Fabric ensures secure transactions and IPFS provides decentralized storage. It uses PoS consensus, MFA and AES-256 encryption to improve security. This trustless yet secure collaboration is driven by the use of blockchain-based federated learning amongst data holders to share healthcare data while retaining privacy. This approach reduces cybersecurity risks, ensures compliance with privacy regulations, and builds a decentralized, privacy-oriented, and cost-effective healthcare landscape.

## 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 Almkadi, 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. Ibrahim, 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. Sherve, 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.