ISSN: 2769-545X

Research Article

Advances in Machine Learning & Artificial Intelligence

Enhancing Federated Learning Security, Scalability, and Future Incentives

Tharwat EL-Sayed[1*], Mohamed Elrashidy[1], Ayman EL-Sayed[1], and Abdullah N. Moustafa[1]

[1]*Computer Science and Engineering, Faculty of Electronic Engineering, 31734, Menoufia, Egypt.a*

[*]**Corresponding Author**
Tharwat EL-Sayed, Computer Science and Engineering, Faculty of Electronic Engineering, Egypt.

Submitted: 2024 Mar 03; **Accepted**: 2024 Mar 25; **Published**: 2024 Apr 08

Citation: EL-Sayed, T., Elrashidy, M., EL-Sayed, A., & Moustafa, A. N. (2024). Enhancing Federated Learning Security, Scalability, and Future Incentives. *Adv Mach Lear Art Inte, 5*(2), 01-07.

Abstract

This study delves into the integration of Storj and blockchain technology within the context of federated learning (FL) and its implications for scalability and efficiency. By leveraging blockchain, we aimed to bolster security and transparency, while also addressing storage challenges through the integration of Incremental Learning. Our findings revealed that while the utilization of Storj led to marginally higher federated server storage requirements compared to local storage, particularly as the number of clients increased, there was also a slight increase in the time required for the federated learning process when Storj was integrated, especially with a larger number of clients.

Keywords: Federated Learning, Blockchain, Storj, People with Special Needs.

1. Introduction

Machine learning is a powerful tool in various fields, including healthcare, but its accuracy depends on having abundant training data. This can raise privacy concerns, especially in healthcare. Regulations like the European Union's General Data Protection Regulation (GDPR) aim to protect user privacy. To address these concerns, researchers are exploring innovative approaches like federated learning and differential privacy. Federated Learning (FL) allows models to be trained on decentralized data sources without compromising privacy, while differential privacy adds noise to training data to protect individual privacy. These techniques aim to strike a balance between accuracy and privacy in healthcare data usage [1].

FL is a distributed machine learning system that allows participants to train models using their local data without sharing it, particularly beneficial in healthcare systems where patient data privacy and security are paramount. FL enables collaborative training using datasets from all participants, leading to improved healthcare decisions and diagnoses while keeping sensitive patient information secure. However, FL faces privacy challenges, as the sharing of model updates between the client and the server can potentially be exploited to reconstruct the client's data. To address this issue, blockchain technology has been proposed as a privacy and security enhancement method for FL in healthcare systems, leveraging the decentralized and immutable nature of blockchain to further enhance privacy protection. However, the implementation of blockchain in FL for healthcare systems requires careful consideration and evaluation to ensure its effectiveness and compatibility with existing infrastructure [2-4].

In the healthcare system, blockchain technology has emerged as a promising solution, used to preserve and exchange patient data across different entities such as hospitals, diagnostic laboratories, pharmacy firms, and physicians. By utilizing a decentralized and secure network, blockchain enhances data accuracy, identifies critical errors in medical records, and improves the performance, security, and transparency of sharing medical data, ensuring that sensitive information remains protected [5]. Additionally, blockchain enables medical institutions to gain valuable insights and enhance the analysis of medical records, leading to more accurate diagnoses, personalized treatments, and advancements in medical research [5]. Overall, the application of blockchain in healthcare has the potential to transform the management and utilization of patient data, ultimately improving healthcare outcomes and patient care.

In traditional FL, a central server aggregates model parameter and distributes the global model, posing a single point of failure susceptible to attacks or crashes [6]. Blockchain integration

addresses this limitation by decentralizing the coordination process, replacing the need for a central server. Each participating device securely uploads its model parameters to the distributed ledger, ensuring accuracy and preventing tampering. The global model is then distributed to all devices in a decentralized manner, eliminating the risk of a single point of failure [7-9]. Blockchain technology offers several strengths when integrated into FL systems. Its architecture, including local data storage, cryptographic algorithms, and immutability, enhances data privacy and security. The transparent nature of blockchain provides visibility into model updates and changes, fostering trust and collaboration among FL system participants. Smart contract automation can enforce data usage policies, ensuring data is shared and utilized under predefined rules and regulations. The immutability and traceability of blockchain make it resistant to illegal tampering attacks, enhancing the security and integrity of the FL process. The combination of FL with blockchain provides a robust and secure framework that resists single points of failure and illegal tampering attacks [10,11].

The use of blockchain and smart contracts in healthcare has the potential to revolutionize the security and accessibility of patient data stored in Electronic Health Records (EHRs). By leveraging blockchain technology, shared health information exchange (HIE) can overcome the limitations of traditional systems and enable universal and secure data sharing among healthcare providers. Blockchain offers a decentralized and transparent approach to protecting patient privacy, replacing the need for a trusted intermediary with cryptographic algorithms that ensure data integrity. However, it's important to note that while blockchain provides strong security measures, complete protection of patient privacy information cannot be guaranteed solely through blockchain technology. The challenges in implementing blockchain technology in healthcare applications, including security, privacy, latency, blockchain size, computing power, storage, scalability, and interoperability, are significant and require further investigation. Security vulnerabilities, privacy concerns, and technical limitations related to data migration, integration, and scalability need to be addressed to ensure the successful adoption of blockchain in healthcare [12]. Overcoming these challenges will require continued research and innovation to fully harness the potential of blockchain technology in healthcare applications and to facilitate collaboration and interoperability within the medical and scientific communities.

There are three main types of blockchains: public blockchains, permissioned or private blockchains, and consortium or federated blockchains. Un-permissioned blockchains, like Bitcoin and Ethereum, allow anyone with internet access to validate transactions and participate in the approval process, aiming to eliminate centralized authority and provide a secure, synchronized transaction ledger. Permissioned blockchains restrict access to authorized companies or organizations, offering higher efficiency in transaction verification and the ability to enforce access controls and data privacy. Participants in a permissioned blockchain can have different levels of access permissions, making them suitable for industries that require strict data confidentiality. However, they lack the decentralization and security of public blockchains. Despite these limitations, permissioned blockchains have gained popularity in various industries due to their ability to provide efficiency, privacy, and controlled access. Consortium blockchains combine elements of private and public blockchains, acting as centralized systems with strong cryptographic models for transaction verification, and their reliability and accuracy are still being explored [12].

Storj is a decentralized cloud storage platform that allows users to store their data in a secure and distributed manner. It uses blockchain technology and a network of nodes to store and retrieve data, providing a more secure and private alternative to traditional cloud storage services [13]. Storj utilizes smart contracts to facilitate the storage and retrieval of data on its decentralized network. Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into code. In the case of Storj, smart contracts are used to automate and enforce the terms of data storage and retrieval between users and storage node operators on the network. This helps ensure the security and reliability of the storage and retrieval process [14].

The rest of this paper is organized as follows, Section 2 covers related work on Federated Learning and the integration of blockchain with it; Section 3 discusses our approach; Section 4 discusses our experiments and collected results 5 concludes this study and discusses future work.

2. Related work

Federated Learning is a powerful approach that allows multiple participants to collaborate on training a shared model without sharing their raw data. This decentralized approach addresses privacy concerns by keeping data secure and private. However, one of the major challenges in FL is ensuring the trustworthiness of the participating devices. Malicious participants or infected data can have significant effects on the model's output, introducing biases or compromising the integrity of the training process. Blockchain technology can play a crucial role in addressing the challenges of trustworthiness, privacy, and fairness in FL. By leveraging the decentralized and transparent nature of blockchain, FL can eliminate the need for intermediaries and create a secure environment for participants to contribute their data [15].

The research of Chang, Fang, and Sun introduced an innovative FL-chain system that incorporates an adaptive differential privacy algorithm specifically designed for the Medical Internet of Things (MIoT) environment [16]. This system addresses the challenge of maintaining a delicate balance between privacy and accuracy by dynamically adjusting the amount of noise added to the gradient. By doing so, the FL-chain system ensures that sensitive medical data remains protected while still achieving accurate model training. A notable strength of this FL-chain system lies in its implementation

of a gradient verification-based consensus protocol. This protocol serves as a robust defense mechanism against malicious attacks and mitigates the risk of a single point of failure. By verifying the gradients contributed by participants, the system ensures the integrity and reliability of the training process, enhancing the overall security of the FL-chain system in the context of MIoT.
Passerat-Palmbach et al. introduced the FL-chain framework, which focuses on privacy preservation in electronic health data to mitigate bias, enhance security, and ensure persistence [17]. This framework consists of six key elements: ”discoverable data and analytic process,” ensuring transparency and traceability; ”fabricated value,” involving the generation of synthetic or fabricated data to protect sensitive information; ”compute guarantees,” ensuring secure and reliable computations; ”privacy guarantees,” implementing privacy-preserving techniques such as differential privacy or secure multi-party computation; ”data quality,” emphasizing the importance of maintaining high-quality data throughout the FL-chain process; and ”collaborative learning,” enabling secure and privacy-preserving machine learning in healthcare. By incorporating these elements, the FL-chain framework provides a comprehensive approach to privacy preservation in electronic health data, addressing the challenges of bias, security, and persistence.

Salim and Park proposed a secure Electronic Health Record (EHR) scheme for hospitals, combining Federated Learning (FL) and blockchain technology [18]. The scheme uses the Interplanetary File System (IPFS) to store private data, ensuring confidentiality and integrity. The IPFS network records hashed addresses of EHRs using a Consortium Blockchain-based network, providing a transparent and tamperproof record of the EHRs. Access to the EHRs is granted to individual patients through smart contracts, ensuring secure and controlled sharing of their medical data. The EHR data is trained both locally and globally, leveraging the power of FL. Local training allows individual hospitals or healthcare providers to train models using their data, preserving data privacy, while global training involves aggregating the locally trained models to create a more robust and accurate global model.
Lakhan et al. conducted a study on fraud detection within the Internet of Medical Things (IoMT) Federated Learning (FL) network [19]. They introduced the FLBETS (Federated Learning Blockchain-Enabled Task Scheduling) framework, which integrates dynamic heuristics to ensure privacy preservation and fraud detection at various stages of data processing. By utilizing blockchain technology, FL-BETS establishes a transparent and tamper-proof record of data transactions, thereby enhancing the security and integrity of the FL network. The framework’s dynamic heuristics enable efficient fraud detection, facilitating the identification of suspicious activities or anomalies in the data.
Guan. explores the application of federated learning (FL) using wearable devices and real leg agility data from Parkinson’s disease (PD) patients [20]. FL is a privacy-preserving approach that allows machine learning models to be trained without compromising the privacy of the underlying data. The study successfully demonstrates that FL can protect sensitive patient data while still achieving reasonably high classification accuracy. It also investigates the effects of interruptions in the FL communication process and the introduction of noise to the model parameters.

The integration of IoT devices onto the Blockchain increases transactions and storage requirements. To address this, Nartey, Clement. proposed a hybrid architecture using containerization to create a side chain on a fog node, and an Advanced Time-variant Multi-objective Particle Swarm Optimization (AT-MOPSO) algorithm to determine optimal block transfers to the cloud [21]. AT-MOPSO incorporates time variant weights and outperforms other algorithms in cloud storage cost and query probability optimization.

Pabitha, P. in his work addresses the challenges faced by IoT networks, such as limited computing power, data security concerns, and scalability issues [22]. To overcome these challenges, the authors propose a hybridized conceptual framework called ModChain. ModChain modifies the structure of blockchain to accommodate the unique requirements of IoT networking. The framework includes a node committee responsible for appending blocks, ensuring fairness in mining, and preventing fraudulent transactions. An incentivization module is defined to discourage the leader of the committee from engaging in fake transactions.
Dwivedi proposed a blockchain-based solution for secure management and analysis of healthcare big data, emphasizing the increasing importance of medical care and the rise of medical big data, as well as the adoption of IoT-based wearable technology in the healthcare sector [23]. The author highlighted the privacy and security risks associated with these technologies and introduced a novel framework of modified blockchain models designed for resource-constrained IoT devices. This framework leverages the distributed nature of IoT devices and incorporates advanced cryptographic primitives to enhance privacy and security. The aim is to ensure secure and anonymous IoT application data and transactions within a blockchain-based network, addressing the privacy and security challenges associated with medical data in the IoT healthcare domain.

2.1 Modifying our proposed model

The main objective of our work is to enhance our FL approach with the integration of blockchain technology. This allowed us to train our Deep Neural Network (DNN) model on decentralized data sources without compromising privacy and security. Our DNN model incorporated a convolutional layer, attention layer, and Bidirectional long shortterm memory (BiLSTM) layer. We applied a FL approach with the help of blockchain to train our DNN model. By leveraging FL, we trained our model on decentralized data sources without transferring the data to a central server, ensuring privacy and security. The incorporation of blockchain technology enhanced transparency and immutability in the training process. Our results demonstrate the effectiveness of this approach in achieving accurate and robust DNN models while maintaining data privacy and security. This research contributes to the field of FL and blockchain applications, offering a promising solution for

collaborative and secure machine learning. Our application aims to improve the communication abilities of individuals with special needs and to assist them in comprehending their environment more effectively.

In our work, we made use of Storj, a decentralized cloud storage platform, and Google Colab, a collaborative environment for running Python code. By leveraging Storj's decentralized storage solution, we were able to explore a novel approach to managing and storing data for our application. Additionally, utilizing Google Colab provided us with a convenient and collaborative platform for running and experimenting with our Python-based code. This combination of technologies allowed us to tap into the benefits of decentralized storage while also taking advantage of a collaborative and efficient development environment. Storj enhances security and privacy through a combination of decentralized storage, client-side encryption, data sharding, access control, and blockchain technology. By distributing data across a network of nodes, Storj reduces the risk of a single point of failure and makes it more resilient to attacks. Client-side encryption ensures that data is encrypted before it leaves the client's device, with only the data owner holding the encryption keys, thus adding an extra layer of security. Data sharding further strengthens security by breaking data into smaller pieces and distributing them across multiple nodes, making unauthorized access more difficult. Access control mechanisms are in place to ensure that only authorized parties can retrieve and modify data stored on the network. Additionally, Storj leverages blockchain technology for managing and enforcing storage contracts, providing a transparent and tamper-resistant record of storage and retrieval activities. This comprehensive approach aims to provide users with a more secure and private cloud storage solution [18]. In our research, we addressed the storage challenge in blockchain by integrating Incremental Learning into the FL process using Storj.

$\hat{\beta}_{ij}$

We successfully updated machine learning models with a more efficient and storage conscious approach by treating the new data as the average weights and the older data as the previous round clients' weights. This method allowed for the streamlined utilization of storage resources within the blockchain environment, as only the average weights needed to be stored, significantly reduced the overall storage requirements. Furthermore, to optimize storage usage, the clients' weights from each round were systematically deleted after calculating the round average weight, ensuring that only essential data was retained, thus addressing the storage constraints typically associated with blockchain-based FL. Leveraging Storj's decentralized and encrypted storage capabilities, combined with this innovative approach to data storage, proved to be an effective solution for overcoming the storage limitations in FL processes within blockchain environments. Expanding the client count in each experiment allows us to assess the scalability of our approach and understand how performance varies with the number of clients involved. Furthermore, comparing the results of experiments with and without the integration of Storj and blockchain enables us to evaluate the impact of these technologies on the FL process. Calculating the duration between the start and end times of each experiment is a reliable way to measure the time taken for each experiment. By comparing the execution times with and without Storj and blockchain, we can gain insights into the impact of these technologies on the overall time required for the FL process.

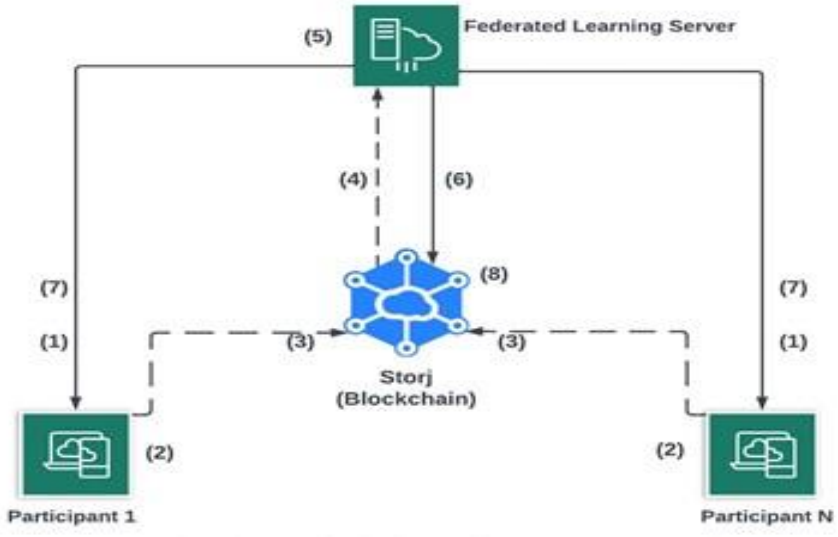

Figure 1: Blockchain-Enabled FL Process Flow.

As illustrated in Figure 1, the combination of FL with blockchain technology involves a meticulously orchestrated series of steps. Initially, the model is initialized by transmitting the initial model from the FL server to the participating clients (1). Subsequently, the participating clients engage in the model learning process (2), followed by the uploading of learning weights from the participating clients to the blockchain (3). The FL server then retrieves round clients' weights from the blockchain (4) and proceeds to calculate the average weight (5), which is subsequently preserved on the blockchain (6). This average weight is then utilized to initiate the next round by deploying the new model with the updated average weights to participating clients (7). Finally, the previous round clients' weights are expunged from the blockchain (8). These iterative processes are iterated multiple times, spanning several rounds, until the desired model performance is achieved.

3. Experiments and Results

We employed k-fold cross-validation with k=5 for dividing the dataset, and conducted 3 learning epochs for each client, repeating the process for 3 rounds. We conducted four experiments to evaluate the performance of our FL approach. Each experiment was run with two options: firstly, without the integration of Storj and blockchain, and secondly, by applying Storj and blockchain. The first experiment involved 3 clients, training the model for 3 rounds and evaluating its performance using various metrics. Building upon this, the second experiment expanded the client count to 5, repeating the FL process and assessing performance using the same metrics, also the third experiment expanded the client count to 7, repeating the FL process and assessing performance using the same metrics. In the fourth experiment, we further increased the client count to 10, executing the FL process for the same number of rounds and comparing the resulting metrics to those obtained previously. To measure the time taken for each experiment, we recorded the start and end times. This allowed us to calculate the duration of each experiment by subtracting the start time from the end time. By comparing the execution times of the experiments with and without Storj and blockchain, we were able to assess the impact of these technologies on the overall time required for the FL process.

Figure 2: Model Learning Time.

As shown in Figure 2, our results showed a slight increase in the time taken for the FL process when Storj was integrated, especially with a larger number of clients. These findings provide valuable insights into the trade-offs between using Storj and local storage in an FL setting, shedding light on the time efficiency of our approach.

To quantify the relationship between the time required for the Federated Learning (FL) process and key factors such as the number of clients and storage type, we employed a linear regression model. The constructed equation is given by

$$Time = \beta_0 + \beta_1 \times \text{Number of Clients} + \beta_2 \times \text{Storage Type} \qquad (1)$$

where β_0 represents the y-intercept, β_1 captures the linear effect of the number of clients on time, and β_2 accounts for the linear effect of the storage type on time (with 1 denoting Storj and 0 denoting local storage).

This simplified model offers a clear representation of the potential impact of these variables on the overall time required for the FL process. While more complex models were considered, the simplicity of this linear equation aligns with the characteristics of our data and allows for straightforward interpretation of the relationships between variables.

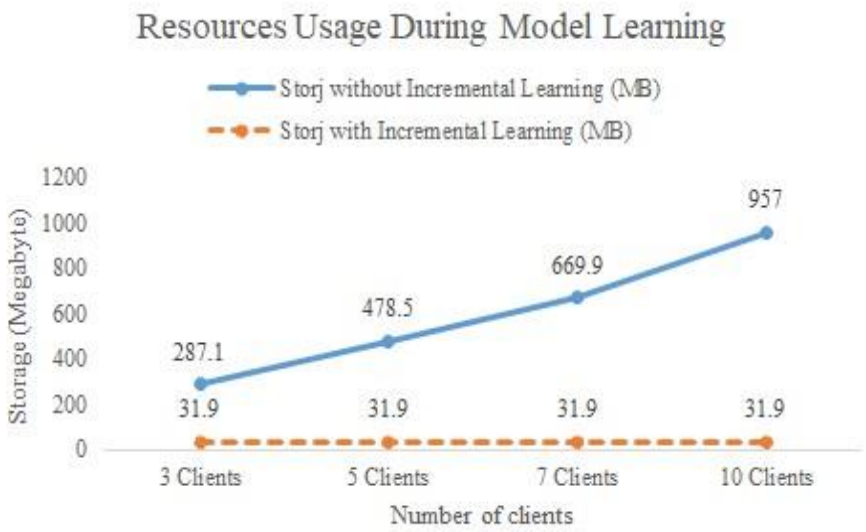

Figure 3: Resources Usage During Model Learning.

Fig.3, shows our resource usage results and reveals a substantial difference in storage requirements between the traditional approach and the integration of Incremental Learning with Storj. Without Incremental Learning, the storage requirements increased significantly as the number of clients grew. However, with Incremental Learning, the storage requirements become small regardless of the number of clients, showcasing a highly efficient and storage-conscious approach. The consistent storage requirements with Incremental Learning, even as the client count increased, underscore the scalability and efficiency of our solution in addressing the storage challenge in FL, particularly within the blockchain environment. These findings highlight the potential of our approach to streamline the utilization of storage resources and overcome the storage limitations typically associated with FL processes. This information is crucial for making informed decisions about the infrastructure and resource allocation for FL systems, ultimately contributing to advancing efficient and scalable FL methodologies.

4. Conclusion and Future Works

Our study has provided valuable insights into the integration of Storj and blockchain technology in the context of FL, demonstrating the potential of blockchain to enhance security and transparency while addressing storage challenges through Incremental Learning integration. The findings underscore the importance of carefully considering the implications of utilizing Storj and blockchain in FL systems, particularly in terms of storage requirements and time efficiency, which are crucial for optimizing performance and scalability. While our results show promise, further research and development are necessary to fully unlock the potential of blockchain technology in FL and address the associated challenges. Continuing to explore and refine the use of blockchain in FL can lead to more secure, efficient, and scalable systems, contributing to advancements in privacy-preserving machine learning and decentralized data processing. Our future work will focus on addressing the challenge of ensuring fairness in FL systems by integrating an incentive mechanism with blockchain technology. This will involve providing benefits such as financial rewards in the form of tokens, data rewards like more precise updates, or other unspecified rewards to participants with varying computational and data resources [14,15]. It is crucial to ensure that those with better resources receive additional benefits to maintain their incentive to contribute, thereby preventing capable participants from losing motivation to further engage in the process.

References

1. McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017, April). Communication-efficient learning of deep networks from decentralized data. In *Artificial intelligence and statistics* (pp. 1273-1282). PMLR.
2. Gu, X., Sabrina, F., Fan, Z., & Sohail, S. (2023). A review of privacy enhancement methods for federated learning in healthcare systems. *International Journal of Environmental Research and Public Health, 20*(15), 6539.
3. Nguyen, D. C., Ding, M., Pham, Q. V., Pathirana, P. N., Le, L. B., Seneviratne, A., ... & Poor, H. V. (2021). Federated learning meets blockchain in edge computing: Opportunities and challenges. *IEEE Internet of Things Journal, 8*(16), 12806-12825.
4. Shayan, M., Fung, C., Yoon, C. J., & Beschastnikh, I. (2020). Biscotti: A blockchain system for private and secure federated learning. *IEEE Transactions on Parallel and Distributed Systems, 32*(7), 1513-1525.
5. Haleem, A., Javaid, M., Singh, R. P., Suman, R., & Rab, S. (2021). Blockchain technology applications in healthcare: An overview. *International Journal of Intelligent Networks, 2*, 130-139.
6. Jiang, S., Lu, M., Hu, K., Wu, J., Li, Y., Weng, L., ... & Lin, H. (2023). Personalized federated learning based on multi-

head attention algorithm. *International Journal of Machine Learning and Cybernetics, 14*(11), 3783-3798.
7. Seneviratne, O. (2022, June). Blockchain for social good: Combating misinformation on the web with AI and blockchain. In *Proceedings of the 14th ACM Web Science Conference 2022* (pp. 435-442).
8. Ali, M., Karimipour, H., & Tariq, M. (2021). Integration of blockchain and federated learning for Internet of Things: Recent advances and future challenges. *Computers & Security, 108,* 102355.
9. Qu, Y., Uddin, M. P., Gan, C., Xiang, Y., Gao, L., & Yearwood, J. (2022). Blockchain-enabled federated learning: A survey. *ACM Computing Surveys, 55*(4), 1-35.
10. Lee, J. Y. (2019). A decentralized token economy: How blockchain and cryptocurrency can revolutionize business. *Business Horizons, 62*(6), 773-784.
11. Wen, J., Zhang, Z., Lan, Y., Cui, Z., Cai, J., & Zhang, W. (2023). A survey on federated learning: challenges and applications. *International Journal of Machine Learning and Cybernetics, 14*(2), 513-535.
12. Hussien, H. M., Yasin, S. M., Udzir, S. N. I., Zaidan, A. A., & Zaidan, B. B. (2019). A systematic review for enabling of develop a blockchain technology in healthcare application: taxonomy, substantially analysis, motivations, challenges, recommendations and future direction. *Journal of medical systems, 43*, 1-35.
13. Li, H., Mi, X., Dou, Y., & Guo, S. (2023, June). An empirical study of storj dcs: Ecosystem, performance, and security. In *2023 IEEE/ACM 31st International Symposium on Quality of Service (IWQoS)* (pp. 1-10). IEEE.
14. Anand, M. V., Mithun, S., Shree, L. D., & Ranjith, M. (2023, January). Survey on connecting to the decentralized storage using IPFS protocol with web 3 technology. In *2023 International Conference for Advancement in Technology (ICONAT)* (pp. 1-4). IEEE.
15. Kapanova, K., Guidi, B., Michienzi, A., & Koidl, K. (2020, September). Evaluating posts on the steemit blockchain: Analysis on topics based on textual cues. In *Proceedings of the 6th EAI international conference on smart objects and technologies for social good* (pp. 163-168).
16. Passerat-Palmbach, J., Farnan, T., McCoy, M., Harris, J. D., Manion, S. T., Flannery, H. L., & Gleim, B. (2020, November). Blockchain-orchestrated machine learning for privacy preserving federated learning in electronic health data. In *2020 IEEE international conference on blockchain (Blockchain)* (pp. 550-555). IEEE.
17. Kumar, A., Kumar, S., & Tyagi, V. (2022, October). Automatic Detection and Monitoring of Hate Speech in Online Multi-social Media. In *International Conference on Advanced Communication and Intelligent Systems* (pp. 605-612). Cham: Springer Nature Switzerland.
18. Salim, M. M., & Park, J. H. (2022). Federated learning-based secure electronic health record sharing scheme in medical informatics. *IEEE Journal of Biomedical and Health Informatics, 27*(2), 617-624.
19. Lakhan, A., Mohammed, M. A., Nedoma, J., Martinek, R., Tiwari, P., Vidyarthi, A., ... & Wang, W. (2022). Federated-learning based privacy preservation and fraud-enabled blockchain IoMT system for healthcare. *IEEE journal of biomedical and health informatics, 27*(2), 664-672.
20. Guan, B., Yu, L., Li, Y., Jia, Z., & Jin, Z. (2023). Assessment of patients with Parkinson's disease based on federated learning. *International Journal of Machine Learning and Cybernetics*, 1-12.
21. Nartey, C., Tchao, E. T., Gadze, J. D., Yeboah-Akowuah, B., Nunoo-Mensah, H., Welte, D., & Sikora, A. (2022). Blockchain-IoT peer device storage optimization using an advanced time-variant multi-objective particle swarm optimization algorithm. *EURASIP Journal on Wireless Communications and Networking, 2022*(1), 5.
22. Pabitha, P., Priya, J. C., Praveen, R., & Jagatheswari, S. (2023). ModChain: a hybridized secure and scaling blockchain framework for IoT environment. *International Journal of Information Technology, 15*(3), 1741-1754.
23. Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2019). A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors, 19*(2), 326.