

BTIMFL: A Blockchain-Based Trust Incentive Mechanism in Federated Learning

Minjung Park and Sangmi Chai(✉)

Ewha Womans University, Seoul, Republic of Korea
{mjpark6767,smchai}@ewha.ac.kr

Abstract. Federated learning (FL) is a machine learning technique that allows multiple devices to train a model collaboratively without sharing their data with a central server. It has advantages such as increased privacy, reduced communication costs, and improved scalability, making it useful in scenarios where data is distributed across multiple devices and privacy is a concern, such as in healthcare or finance. However, the potential for participants to behave selfishly in FL can be a challenge, and incentive mechanisms are needed to encourage them to participate in the training process. Incentives can take many strategies, such as financial rewards or reputation-based systems, and can be tailored to specific needs. In defense technology, FL can be used for predictive maintenance, target recognition, and intelligence analysis. However, the existing incentive mechanisms in FL have limitations, such as being complex to design and implement, and raising privacy concerns. To improve the incentive mechanisms in FL, we propose an incentive mechanism based on blockchain called BTIMFL that ensures transparency and effectiveness. The proposed mechanism includes DAO (Decentralized Autonomous Organizations) and smart contracts for the automatic distribution of profits to ensure fairness.

Keywords: Blockchain · DAO (Decentralized Autonomous Organizations) · Federated Learning (FL) · Inventive Mechanism · Smart Contracts

1 Introduction

Federated learning (FL) is a machine learning technique that allows multiple devices to collaboratively train a model without having to share their data with a central server [1–6]. Instead of sending data from individual devices to a central location for analysis, FL allows the data to remain on each device, while the model is sent to each device for training [4, 7, 8]. The updated model weights are then sent back to a central server where they are aggregated and used to improve the model. It has several advantages, including increased privacy for the data owners, reduced communication costs, and improved scalability. It is especially useful in scenarios where data is distributed across multiple devices and cannot be easily transferred to a central location for analysis, such as in the case of mobile devices, Internet of Things (IoT) devices, or healthcare devices [9–11]. It can also be used in cases where data privacy is a concern, such as in the medical or financial industries [5].

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2023
O. Gervasi et al. (Eds.): ICCSA 2023 Workshops, LNCS 14106, pp. 175–185, 2023.
https://doi.org/10.1007/978-3-031-37111-0_13

Incentive mechanisms are important in FL because they encourage participants to contribute their data and computational resources to the FL process. Since FL involves training models on data that is distributed across multiple devices, it is important to incentivize these devices to participate in the training process proactively [6, 12, 13]. A key challenge with FL is the potential for participants to behave greedily, either by refusing to contribute their data or by intentionally sending incorrect data to the central server [5]. Incentive mechanisms can be used to address these challenges by rewarding participants for contributing high-quality data and penalizing them for misbehavior [5]. Effective incentive mechanisms can help ensure that participants have an incentive to contribute to the FL process and are motivated to do so in a way that benefits the overall training objective [5, 6]. Incentives can take many forms, such as financial rewards, reputation-based systems, or other forms of recognition, and they can be tailored to the specific needs of its application. Especially, in defense technology, FL can be used for a variety of purposes. In the defense industry, predictive maintenance is critical to ensuring that equipment and machinery are operating efficiently and effectively. FL can be used to train predictive maintenance models on distributed datasets from different units, enabling better predictions and maintenance scheduling. It can also be used for target recognition in defense applications. For example, drones equipped with cameras can collect images of potential targets, which can be analyzed and classified using federated learning algorithms. The models can be trained on distributed datasets from different drones, improving the accuracy of target recognition while preserving data privacy. FL may help to train models for intelligence analysis, such as natural language processing models for analyzing text data. It can be used to analyze distributed datasets of intelligence reports, enabling better insights while preserving the privacy of sensitive data. Overall, FL has great potential in defense technology applications, enabling better machine learning models while preserving data privacy and security. In summary, incentive mechanisms are important in FL because they help address the challenges of data distribution and self-interested behavior among participants, and they can help ensure the success of its process. Therefore, a lot of studies have performed to design incentive mechanism for operated FL effectively.

It is identified that the existed incentive mechanism in FL has some limitations that should be solved. First, incentive mechanisms can be expensive to implement, particularly if they involve financial rewards or other forms of compensation [14]. The cost of implementing these mechanisms can sometimes outweigh the benefits, particularly if the FL project is relatively small or has limited resources. Secondly, incentive mechanisms can be complex to design and implement, particularly if they involve a large number of participants or require sophisticated algorithms to calculate rewards or penalties [9]. This complexity can make it difficult to ensure that the incentives are fair, transparent, and effective [15]. Third, it raises privacy concerns, particularly if they involve the exchange of sensitive information or the tracking of participant behavior [16, 17]. It can generate a refuse of participation with privacy concerns, which may be difficult to resolve. It is important to carefully consider the potential limitations and tradeoffs involved in implementing FL successfully [18]. Therefore, this study suggests the incentive mechanism with adopting blockchain (i.e., BTIMFL) for improving its transparency and effectiveness compared to existing incentive mechanism.

The main contributions of this paper are as follows: 1. We comprehensively consider prior research on incentive mechanisms adopted by FL to derive features and improvements. 2. To improve incentive mechanism of FL, we propose an incentive mechanism based on blockchain. The decentralization of the blockchain cannot be tampered with, so it can prevent the local model parameters from being tampered with and affecting the overall model performance. 3. We suggest an incentive mechanism based on smart contracts and DAO (Decentralized Autonomous Organization). Participants who contribute to the model will be rewarded to ensure the sustainable development of FL. To ensure the fairness of incentives, we have designed a smart contract for the automatic distribution of profits on the blockchain that avoids the participation of third parties.

2 Related Works

2.1 Federated Learning

FL is a new distributed machine learning technique that allows multiple devices or machines to collaboratively train a model without sharing their data with each other [2, 3, 8, 19]. In FL, a central server coordinates the learning process, but the data remains on the local devices such as smartphone [17, 18]. The devices perform the computation on their own data and then send the model updates to the central server [2, 17]. The central server aggregates these updates to create an improved global model, which is then sent back to the devices to be further refined [8, 19].

FL allows for the training of models without centralizing sensitive data [20]. It has been developed to address the privacy concerns associated with centralized machine learning [14, 20]. In traditional machine learning, data is centralized on a server, and the model is trained, however, centralized data on a server raises privacy concerns since the data may contain sensitive or personal information [1, 19]. Additionally, transmitting large amounts of data to a centralized server may increase the risk of data breaches [18]. The most data have no choice but to be stored across multiple devices or locations, making it difficult or impossible to avoid centralize the data for training [2, 18]. FL can enable training on edge devices, where the data is generated, reducing the need for centralized computation [19]. It is well-suited for cases where the data is sensitive or where the data volume is too large to be sent to a centralized server for training.

FL is a rapidly evolving area of research and is being applied in many fields, including finance, healthcare, and natural language processing. FL has been used in mobile device applications to improve predictive text, auto-correction, and voice recognition. For example, the Google keyboard (Gboard), uses FL to personalize typing suggestions based on the user's writing style [14]. It also has been used in healthcare to develop models for diagnosing diseases, predicting outcomes, and identifying potential drug targets. Researchers have used FL to train models for detecting diabetic retinopathy by aggregating data from different healthcare institutions without centralizing patient data [20].

FL is widely adopted not only for privacy-preserving, but also for scalability and efficiency. FL enables the training of models using decentralized computing resources, which makes it possible to scale machine learning to massive datasets [21, 22]. By training models locally, FL can reduce the need for large centralized data storage and

processing and large amounts of data to be transmitted to a central server, which can save time and resources [23, 24]. In other words, it can improve efficiency by saving time, bandwidth, and computing resources.

FL is a rapidly evolving research area with many developments and opportunities and recent research trends are summarized as follows. First, privacy and security is the main challenges of FL which ensure the data privacy and security. Recent research has mainly focused on developing techniques for secure aggregation, differential privacy (DP) [25–27], and homomorphic encryption (HE) [16, 28, 29] to protect the privacy of user data while allowing for effective model training. Second, FL often requires communication between devices, which can be a bottleneck in the training process. It can result in increased latency, network congestion, and reduced model training efficiency when dealing with large amounts of data [23, 30]. Therefore, recent research has focused on securing communication-efficient algorithms with developing algorithms that minimize communication overhead while still achieving high model accuracy. For example, to reduce the communication overhead by aggregating global model only when the global model's weight differed by some selected threshold is suggested [8]. Third, FL can be applied to a wide range of data sources, including text, images, audios, and sensor data. Almost, FL algorithms assume that data is homogeneously distributed across devices, however, the data may be highly heterogeneous, in real-world, which can lead to issues such as imbalanced datasets, noisy data, and biased training [31, 32]. It addresses the needs for exploring the challenges of training models on heterogeneous data sources and develops techniques for adapting models to different types of data. To mitigate the effect of non-independent and non-identically data, a feature fusion approach by aggregating local and global model is presented [33]. Similarly, it is designed to form clusters of clients based on the geometrics properties of the FL surface with jointly trainable data distribution. Fourth, FL systems are vulnerable to various attacks, such as poisoning attacks, model inversion attacks, and membership inference attacks [34–36]. Therefore a few studies have focused on developing algorithms that are robust to attacks.

2.2 Incentive Mechanism for Federated Learning

Incentive mechanisms are used in FL to incentivize the participants to contribute their data and computational resources to the training process. Without proper incentives, participants may not be willing to contribute their resources, leading to a lack of participation and finally, lower model performance [1–3, 8, 19, 24]. The importance of incentive mechanism in FL can be summarized as follows. First, in FL, it may collect varied computational resources of participants. Participants may be unwilling to share those resources without proper incentives because they have limited computational resources [2]. Secondly, recent users have be-gun to perceive the 'data ownership' of the data they have generated or data about themselves (i.e., personal information) and consider it as their own property. There-fore, participants may be reluctant to share it without proper incentives, which could result in a limited and biased dataset [37, 38]. It can help increase participation in the training process by providing participants with an incentive to contribute their high-quality data [1, 3]. An incentive mechanism can finally encourage participants to contribute high-quality data, leading to higher model performance. Third, incentive mechanisms can help ensure that participants are compensated fairly

for their contributions [4, 9]. This can help prevent participants from feeling exploited and can lead to greater participation in future training rounds [39]. Overall, incentive mechanisms are important in FL because they can help to promote greater participation, higher-quality contributions, and better privacy and security protections for participants. It is possible to achieve the desired outcomes while minimizing negative impacts on participants by designing incentive mechanisms effectively.

Based on the importance of the incentive mechanism in FL, a few studies have designed it with considering the following principles: fairness, privacy, transparency, flexibility. Incentive mechanisms should be designed to be fair to all participants. It means that the rewards should be proportional to the contributions made by each participant and should not unfairly favor any participant or groups. Incentive mechanisms also should not compromise the privacy or security of the participants' data. Participants understand how the rewards are estimated and what they need to do to earn them by securing its transparency. It can help to build trust and encourage participation. Incentive mechanisms has to be flexible, so that they can adapt to changing conditions or goals. The rewards should be adjustable based on the needs of the system and should not be fixed or static.

The goal of embedding incentive mechanism is to motivate participants to contribute in FL and improve the performance of it. The optimal strategy of each participant and the reward of the server are determined through solving the optimization problems (e.g., social welfare maximization problem) in the incentive mechanism. The reward paid to each participant is allocated according to the contribution measurement, node selection and payment allocation with three phase levels [10]. The objective of contribution measurement is to fairly evaluate each participant's contribution to FL training performance, which includes various resources beyond just training data [40]. Node selection involves choosing a subset of participants with enough resources that fit within the system's budget constraints. It is important to consider different types of resources to ensure efficient training, as a participant with low computing power and ample data may cause delays [41]. Payment allocation involves deciding how to distribute payments to participants, which may include money, usage of the global model, and other rewards. Payment allocation problems are difficult to solve, and it is essential to find efficient solutions [7]. These components should be interdependent [10]. A lot of studies adopted various economic and game theoretic approaches to design incentive mechanism, including Stackelberg game, Shapley value, auction, contract theory, and reinforcement learning.

Stackelberg Game. Stackelberg game can be used to incentivize participation in FL by providing additional rewards or benefits to the first mover or leader [10]. By encouraging a leader to initiate the learning process and share the learned model with others, Stackelberg game can promote cooperation and participation among other entities [42]. It assumes that there is a clear distinction between the leader and the followers, which may not be applicable in all FL scenarios [10]. Additionally, the leader may not always act in the best interest of the overall learning process, particularly if their incentives are misaligned with the goals of the others [10].

Shapley Value. Shapley Value can be adopted to determine the fair allocation of rewards among participating entities based on their contributions to the overall model accuracy in FL [10, 11]. Shapley Value provides a way to fairly distribute rewards and incentivize participation by considering the marginal contribution of each entity [5]. It assumes that

the contributions of each entity are independent and additive, which may not always be the case in FL [9]. Computing the Shapley Value can be computationally expensive, in scenarios with a large number of participating entities.

Auction. Auction mechanisms can be applied with incentive mechanism to allocate resources such as computation or communication bandwidth among participating entities. By creating a competitive environment, auction mechanisms incentivize entities to bid for resources and provide accurate model updates in exchange for higher rewards [10]. Auction mechanisms require a clear and well-defined set of resources to be auctioned, which may not be feasible in all FL scenarios. The auction process can be vulnerable to manipulation or collusion by participating entities, which can compromise the fairness of the allocation.

Contract Theory. Contract theory can be used to design incentive mechanisms in FL that align the interests of participating entities with the overall goals of the learning process [5]. To create contracts that specify the rewards and penalties for different behaviors, contract theory can incentivize entities to behave in ways that maximize the overall learning performance [1, 6, 13]. Contract theory assumes that there is a clear and complete understanding of the learning process and the behavior of participating entities, which may not always be the case in FL [10, 24]. To design contracts that incentivize desirable behavior while avoiding unintended consequences can be challenging [6].

Reinforcement Learning. Reinforcement learning can be applied to design adaptive incentive mechanisms in FL that learn and adjust based on the behavior of participating entities [9–11]. By modeling the learning process as a reinforcement learning problem, incentive mechanisms can be designed to encourage entities to behave in ways that maximize the overall learning performance over time [3, 11]. Reinforcement learning requires a well-defined objective function and reward signal, which may not be straightforward to specify in all FL scenarios [10]. Designing an incentive mechanism based on reinforcement learning that balances exploration with attempting to discover new features by a selecting sub-optimal action and exploitation of using what we already know to get the best results we know of can be difficult [43].

The recent limitations of incentive mechanisms in FL is the challenge of designing it that are resistant to various types of attacks and malicious behaviors. One of the major examples is the "free-riding" problem, where some entities may withhold their data or provide low-quality updates in order to receive the benefits of FL without incurring the costs of participation [44]. Incentive mechanisms need to be designed in a way that encourages participation and contribution from all entities, while also detecting and penalizing free-riding behavior. Another challenge is ensuring the privacy and security of data in FL. Incentive mechanisms need to be designed in a way to ensure the participating entities are not able to access or manipulate sensitive data, while still providing appropriate incentives for collaboration. Finally, there is a need for incentive mechanisms that can adapt to changing conditions and dynamics in FL [5, 13]. For example, as the number and distribution of participating entities changes over time, incentive mechanisms need to be able to adjust the rewards and penalties to maintain a balanced and effective learning process [10]. Addressing as we mentioned and other recent limitations will require continued research and development in the design of incentive mechanisms

for FL, as well as the integration of techniques from areas such as privacy-preserving machine learning, game theory, and distributed systems.

3 Proposed Model

Designing incentive mechanisms in FL using blockchain technology can provide several benefits, such as increased transparency, accountability, and security [14, 18, 22, 45]. Recent studies have explored the use of blockchain in FL for designing incentive mechanisms and some of the key findings could be summarized as follows. First, blockchain can enable decentralized governance mechanisms for FL incentive design. Qu, Gao, Luan, Xiang, Yu, Li and Zheng [46] proposed a blockchain-based governance framework for FL that incorporates reputation-based incentives about reward distribution. Second, blockchain can facilitate privacy-preserving incentive mechanisms in FL [14, 22]. A recent study suggested a blockchain-based framework that uses secure multi-party computation (MPC) to compute rewards without revealing sensitive data [47]. Third, blockchain can enable token-based incentives in FL, where participants are rewarded with cryptocurrency tokens for their contributions and inspire their proactive participants [48]. A token-based incentive mechanism for FL is suggested that leverages smart contracts to enforce rewards and penalties [49, 50]. Fourth, blockchain can support game-theoretic incentive mechanisms in FL. Finally, blockchain can enhance fairness and transparency in FL incentive design. A blockchain-based mechanism that uses fairness measures to ensure that rewards are distributed equitably among participants, while also providing transparency through a public ledger of reward transactions [14, 17, 18, 22, 45, 46, 50]. Overall, these studies demonstrate the potential for blockchain to enhance incentive mechanism design in FL, by enabling decentralized governance, privacy-preserving incentives, token-based rewards, game-theoretic mechanisms, and increased fairness and transparency. However, there is still much research to be performed to fully consider the opportunities and challenges of using blockchain in FL incentive design. Therefore, this study considers the principles of 'smart contracts', 'decentralized governance', 'reputation-based incentives' to design incentive mechanism based on blockchain.

Smart Contracts. Smart contracts can create automated agreements between participants in FL [51, 52]. For example, a smart contract could specify the terms of a data sharing agreement, including the rewards and penalties for each participant based on their contributions. The use of blockchain can ensure that the terms of the smart contract are enforced in a secure and transparent way [50].

Decentralized Governance. Blockchain-based governance (i.e., DAO) mechanisms can be used to ensure that participants have a authority in the decision-making process of the FL system [14]. DAO could be created to manage the incentives and rewards for FL participants [53]. It can ensure that the governance process is transparent and democratic, with each entity having an equal authority in the decision-making process.

Reputation-Based Incentives. Participations are rewarded based on their reputation or track record of providing accurate and high-quality updates [1, 54]. Reputation scores

are maintained in a secure and transparent manner, with each update being recorded on the blockchain [55].

Based on those above-mentioned principles, we suggest the incentive mechanism based on blockchain with trust, called BTIMFL. It fulfills the goals of operating an incentive mechanism with trust: 1) estimating reasonable rewards to all participants and operators of FL, 2) encouraging voluntary participation, and 3) fair distribution of rewards. BTIMFL promotes transparency and fairness in the measurement of rewards for participants based on the operating model of DAOs unlike the mechanisms proposed in the past. In other words, if the existing incentive mechanisms exclusively operate the calculation of rewards on a central server and distribute rewards from the top-down, BTIMFL not only provides data and resources to the FL the moment participants decide to participate in the FL, but also acts as a decision-making entity to evaluate the objectivity of the reward calculation.

In BRIMFL, the specific incentive reward design and distribution process is as follows: First, a user who participates in the FL has the obligation to provide data and resources, as well as the right to be provided incentives for what they provide; second, before providing data and resources, the participant transmits to the block-chain server the amount the participant wants to be compensated for. Third, all participants will view the estimated rewards of all participants through the blockchain and vote on the appropriateness of each reward. Fourth, for each FL, only participants who are approved according to the pre-agreed ratio of votes passed will provide the data and resources they have presented in advance. Fifth, when a participant's data and resource is provided, a ratio of the reward which was consented is sent to each participant according to the smart contract. Finally, the participant who received the reward will receive the entire remaining incentive if the participant is evaluated through the blockchain-based reputation system as a participant who has fulfilled all the pre-agreed conditions, rather than a free rider or a node with negligence of duty.

4 Conclusion

A novel incentive mechanism (i.e., BTIMFL) based on reputation points has been created by combining FL and blockchain technology. The main objective of this study is to establish a trustworthy environment for participation and an automated revenue sharing mechanism. To prevent malicious nodes from causing damage to the global model parameters, this incentive mechanism incorporates reputation points. Nodes with low reputation points are identified as malicious and prohibited from sharing or incorporating in a global model, thereby protecting the global model. It allows more enthusiastic participants to join the federated ecosystem. The increase in data volume enhances the model's effectiveness and enables participants to receive more benefits, resulting in a mutually beneficial outcome with achieving a win-win situation.

This research provides the following future research directions. First, we will verify how the incentive mechanism proposed in this study improves FL operations compared to existing incentive mechanisms from a comprehensive perspective of privacy, communication cost, and scalability. Second, we will further design incentive mechanisms from the perspective of VFL (vertical federated learning) and cross-device. Most of

the existing research on incentive mechanisms is centered on the server to utilize the client's resources with minimal incentive cost in a perspective of cross-silo. Therefore, based on the incentive mechanism proposed in this study, we plan to investigate continuously how to improve a fair and reasonable reward/evaluation system for voluntary client participation in FL in future studies.

References

1. Kang, J., Xiong, Z., Niyato, D., Xie, S., Zhang, J.: Incentive mechanism for reliable federated learning: a joint optimization approach to combining reputation and contract theory. IEEE Internet Things J. **6**, 10700–10714 (2019)
2. Khan, L.U., et al.: Federated learning for edge networks: resource optimization and incentive mechanism. IEEE Commun. Mag. **58**, 88–93 (2020)
3. Zhan, Y., Li, P., Qu, Z., Zeng, D., Guo, S.: A learning-based incentive mechanism for federated learning. IEEE Internet Things J. **7**, 6360–6368 (2020)
4. Yu, H., et al.: A fairness-aware incentive scheme for federated learning. In: Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society, pp. 393–399 (2020)
5. Yan, Y., Ligeti, P.: A survey of personalized and incentive mechanisms for federated learning. In: 2022 IEEE 2nd Conference on Information Technology and Data Science (CITDS), pp. 324–329. IEEE (2022)
6. Liu, Y., Tian, M., Chen, Y., Xiong, Z., Leung, C., Miao, C.: A contract theory based incentive mechanism for federated learning. Federated and Transfer Learning, pp. 117–137. Springer (2022). https://doi.org/10.1007/978-3-031-11748-0_6
7. Zeng, R., Zhang, S., Wang, J., Chu, X.: Fmore: an incentive scheme of multi-dimensional auction for federated learning in mec. In: 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS), pp. 278–288. IEEE (2020)
8. Zhan, Y., Li, P., Guo, S., Qu, Z.: Incentive mechanism design for federated learning: challenges and opportunities. IEEE Network **35**, 310–317 (2021)
9. Shi, Z., et al.: FedFAIM: a model performance-based fair incentive mechanism for federated learning. IEEE Transactions on Big Data (2022)
10. Zeng, R., Zeng, C., Wang, X., Li, B., Chu, X.: Incentive mechanisms in federated learning and a game-theoretical approach. IEEE Network **36**, 229–235 (2022)
11. Yang, X., Tan, W., Peng, C., Xiang, S., Niu, K.: Federated learning incentive mechanism design via enhanced shapley value method. Wireless Communications and Mobile Computing 2022 (2022)
12. Yang, C., Liu, J., Sun, H., Li, T., Li, Z.: WTDP-shapley: efficient and effective incentive mechanism in federated learning for intelligent safety inspection. IEEE Transactions on Big Data (2022)
13. Li, L., Yu, X., Cai, X., He, X., Liu, Y.: Contract theory based incentive mechanism for federated learning in health CrowdSensing. IEEE Internet of Things Journal (2022)
14. Zhu, J., Cao, J., Saxena, D., Jiang, S., Ferradi, H.: Blockchain-empowered federated learning: challenges, solutions, and future directions. ACM Comput. Surv. **55**, 1–31 (2023)
15. Maumela, T., Nelwamondo, F., Marwala, T.: Population based training and federated learning frameworks for hyperparameter optimisation and ML unfairness using ulimisana optimisation algorithm. Inf. Sci. **612**, 132–150 (2022)
16. Ma, J., Naas, S.A., Sigg, S., Lyu, X.: Privacy-preserving federated learning based on multi-key homomorphic encryption. Int. J. Intell. Syst. **37**, 5880–5901 (2022)
17. Singh, S.K., Yang, L.T., Park, J.H.: FusionFedBlock: Fusion of blockchain and federated learning to preserve privacy in industry 5.0. Information Fusion **90**, 233–240 (2023)

18. Issa, W., Moustafa, N., Turnbull, B., Sohrabi, N., Tari, Z.: Blockchain-based federated learning for securing internet of things: a comprehensive survey. ACM Comput. Surv. **55**, 1–43 (2023)
19. Zhan, Y., Zhang, J., Hong, Z., Wu, L., Li, P., Guo, S.: A survey of incentive mechanism design for federated learning. IEEE Trans. Emerg. Top. Comput. **10**, 1035–1044 (2021)
20. Qayyum, A., Janjua, M.U., Qadir, J.: Making federated learning robust to adversarial attacks by learning data and model association. Comput. Secur. **121**, 102827 (2022)
21. Huba, D., et al.: Papaya: Practical, private, and scalable federated learning. Proc. Machine Learning Syst. **4**, 814–832 (2022)
22. Abubaker, Z., Javaid, N., Almogren, A., Akbar, M., Zuair, M., Ben-Othman, J.: Blockchained service provisioning and malicious node detection via federated learning in scalable Internet of Sensor Things networks. Comput. Netw. **204**, 108691 (2022)
23. Pouriyeh, S., et al.: Secure smart communication efficiency in federated learning: achievements and challenges. Appl. Sci. **12**, 8980 (2022)
24. Tu, X., Zhu, K., Luong, N.C., Niyato, D., Zhang, Y., Li, J.: Incentive mechanisms for federated learning: from economic and game theoretic perspective. IEEE Transactions on Cognitive Communications and Networking (2022)
25. Hu, R., Guo, Y., Li, H., Pei, Q., Gong, Y.: Personalized federated learning with differential privacy. IEEE Internet Things J. **7**, 9530–9539 (2020)
26. Seif, M., Tandon, R., Li, M.: Wireless federated learning with local differential privacy. In: 2020 IEEE International Symposium on Information Theory (ISIT), pp. 2604–2609. IEEE (2020)
27. Wei, K., et al.: Federated learning with differential privacy: algorithms and performance analysis. IEEE Trans. Inf. Forensics Secur. **15**, 3454–3469 (2020)
28. Fang, H., Qian, Q.: Privacy preserving machine learning with homomorphic encryption and federated learning. Future Internet **13**, 94 (2021)
29. Zhang, C., Li, S., Xia, J., Wang, W., Yan, F., Liu, Y.: Batchcrypt: Efficient homomorphic encryption for cross-silo federated learning. In: Proceedings of the 2020 USENIX Annual Technical Conference (USENIX ATC 2020) (2020)
30. Shahid, O., Pouriyeh, S., Parizi, R.M., Sheng, Q.Z., Srivastava, G., Zhao, L.: Communication efficiency in federated learning: Achievements and challenges. arXiv preprint arXiv:2107.10996 (2021)
31. Huang, W., Ye, M., Du, B.: Learn from others and be yourself in heterogeneous federated learning. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 10143–10153 (2022)
32. Li, T., Sahu, A.K., Talwalkar, A., Smith, V.: Federated learning: challenges, methods, and future directions. IEEE Signal Process. Mag. **37**, 50–60 (2020)
33. Huang, Y., et al.: Personalized cross-silo federated learning on non-iid data. In: Proceedings of the AAAI Conference on Artificial Intelligence, pp. 7865–7873 (2021)
34. Zhang, X., Gu, H., Fan, L., Chen, K., Yang, Q.: No free lunch theorem for security and utility in federated learning. ACM Trans. Intelligent Syst. Technol. **14**, 1–35 (2022)
35. Gosselin, R., Vieu, L., Loukil, F., Benoit, A.: Privacy and security in federated learning: a survey. Appl. Sci. **12**, 9901 (2022)
36. Rodríguez-Barroso, N., Jiménez-López, D., Luzón, M.V., Herrera, F., Martínez-Cámara, E.: Survey on federated learning threats: concepts, taxonomy on attacks and defences, experimental study and challenges. Information Fusion **90**, 148–173 (2023)
37. Lim, W.Y.B., et al.: Decentralized edge intelligence: a dynamic resource allocation framework for hierarchical federated learning. IEEE Trans. Parallel Distrib. Syst. **33**, 536–550 (2021)
38. Huang, J., Talbi, R., Zhao, Z., Boucchenak, S., Chen, L.Y., Roos, S.: An exploratory analysis on users' contributions in federated learning. In: 2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), pp. 20–29. IEEE (2020)

39. Sarikaya, Y., Ercetin, O.: Motivating workers in federated learning: a stackelberg game perspective. IEEE Networking Letters **2**, 23–27 (2019)
40. Zhao, J., Zhu, X., Wang, J., Xiao, J.: Efficient client contribution evaluation for horizontal federated learning. In: ICASSP 2021–2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 3060–3064. IEEE (2021)
41. Tang, M., Wong, V.W.: An incentive mechanism for cross-silo federated learning: a public goods perspective. In: IEEE INFOCOM 2021-IEEE Conference on Computer Communications, pp. 1–10. IEEE (2021)
42. Wu, H., Tang, X., Zhang, Y.-J.A., Gao, L.: Incentive mechanism for federated learning based on random client sampling. In: 2022 IEEE Globecom Workshops (GC Wkshps), pp. 1640–1645. IEEE (2022)
43. Mai, T., Yao, H., Xu, J., Zhang, N., Liu, Q., Guo, S.: Automatic double-auction mechanism for federated learning service market in internet of things. IEEE Trans. Network Science Eng. **9**, 3123–3135 (2022)
44. Karimireddy, S.P., Guo, W., Jordan, M.I.: Mechanisms that Incentivize Data Sharing in Federated Learning. arXiv preprint arXiv:2207.04557 (2022)
45. Lax, G., Russo, A., Fascì, L.S.: A Blockchain-based approach for matching desired and real privacy settings of social network users. Inf. Sci. **557**, 220–235 (2021)
46. Qu, Y., et al.: Decentralized privacy using blockchain-enabled federated learning in fog computing. IEEE Internet Things J. **7**, 5171–5183 (2020)
47. Mugunthan, V., Rahman, R., Kagal, L.: Blockflow: An Accountable and Privacy-Preserving Solution for Federated Learning. arXiv preprint arXiv:2007.03856 (2020)
48. Han, J., et al.: Tiff: tokenized incentive for federated learning. In: 2022 IEEE 15th International Conference on Cloud Computing (CLOUD), pp. 407–416. IEEE (2022)
49. Qi, M., Wang, Z., Chen, S., Xiang, Y.: A hybrid incentive mechanism for decentralized federated learning. Distributed Ledger Technol.: Res. Practice **1**, 1–15 (2022)
50. Xu, Y., et al.: Besifl: Blockchain empowered secure and incentive federated learning paradigm in iot. IEEE Internet of Things J. (2021)
51. Short, A.R., Leligou, H.C., Theocharis, E.: Execution of a Federated Learning process within a smart contract. In: 2021 IEEE International Conference on Consumer Electronics (ICCE), pp. 1–4. IEEE (2021)
52. Hua, G., Zhu, L., Wu, J., Shen, C., Zhou, L., Lin, Q.: Blockchain-based federated learning for intelligent control in heavy haul railway. IEEE Access **8**, 176830–176839 (2020)
53. Cao, L.: Non-IID federated learning. IEEE Intell. Syst. **37**, 14–15 (2022)
54. Buyukates, B., et al.: Proof-of-Contribution-Based Design for Collaborative Machine Learning on Blockchain. arXiv preprint arXiv:2302.14031 (2023)
55. Rehman, M.H., Salah, K., Damiani, E., Svetinovic, D.: Towards blockchain-based reputation-aware federated learning. In: IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 183–188. IEEE (2020)