Blockchain-Enabled Personalized Federated Learning for Autonomous Vehicles

Pradyumna Kumar Tripathy[1], Weiwei Jiang[2]
[1]Lincoln University College, Malaysia
[1]Associate Professor, Silicon University, Odisha
[2]Associate Professor, The School of Information and Communication Engineering,
Beijing University of Posts and Telecommunications
[1]Email:pdf.Pradyumna@lincoln.edu.my
[2]Email:jww@bupt.edu.cn

Abstract: Modern self-driving autonomous vehicle (AV) biomes need artificial intelligence (AI) structures that are adaptable, strong, and safeguard clients' confidentiality to provide decentralized and distributed privacy-preserving machine learning across various manufacturers' edge devices and cloud environments. With conventional machine learning techniques, confidential vehicle details are transferred and stored in a central server, which affects insignificant reliability and seclusion concerns. This problem is addressed by federated learning (FL), which enables distributed model training instead of attempting to transfer data directly. Despite this FL is still at risk for vulnerabilities like model poisoning attacks, its limited customization options, its dependence on centralized aggregation techniques. This paper introduces a block chain-based personalized federated learning (BPFL) framework that uses distributed server edges, cloud-level collectors, plus smart contractors to ensure proxy-based monitoring to overcome the limitations. Secure model interchange, distributed trust control, tamper-proof secure verification, and personalization across various AV settings are all made possible by proposed architecture. Integration with block chain improves transparency, guarantees security, and strengthens against malicious manipulation. Several experimental tests shows that the proposed BPFL framework significantly enhances resistance to malicious updates and produces better global model performance with an accuracy of 94.2% while reducing communication overhead by 23% when compared to standard FL strategies.

Keywords: federated learning, autonomous vehicle, block chain, edge processing, secure aggregation.

Introduction

Autonomous vehicles continuously generate large-scale multimodal sensor and perception data that demand adaptive and intelligent model training to maintain safe and reliable

operation. Considering these types of scenarios, classic centralized learning paradigms are insufficient because of strict privacy regulations, high communication bandwidth needs, and latency limits. These issues are addressed through federated learning(FL)[1]. Which permits collaborative model training among distributed clients while maintaining data localization, especially confidentiality via avoiding revealing the initial information. Despite its advantages, current FL systems rely on a centralized aggregation server, which leads to basic confidence reliance and susceptibility to single-point failures and limited transparency in model verification processes [2]. Also, statistical variability and non-IID data from various manufacturers and driving situations considerably impede global convergence and diminish the efficacy of personalization [3]. Decentralized trust management, immutability, audibility, and safe transaction validation via distributed consensus processes are all introduced by block chain technology [4]. By integrating block chain with FL, system transparency is increased, tamper-resistant model update tracking is made possible, and robustness against malevolent or Byzantine actors is strengthened [5]. The need for safe aggregation methods [6], differential privacy techniques [7], and Byzantine resilient optimization methodologies [8] to reduce the risk of model poisoning and adversarial manipulation in collaborative learning environments is further highlighted by recent works. Additionally, it has been shown that layered and edge-enabled collaborative design improves communications effectiveness and scalability across large-scale distributed computing systems [9]. This study improves the block chain-integrated personalized federated learning framework created especially for autonomous vehicle ecosystems in response to these problems. The proposed method combines decentralized trust enforcement through unchangeable block chain registration and smart-contract-based verification approaches to achieve safe and dependable model aggregation. In order to successfully handle heterogeneous and non-IID data distributions across participants, it integrates personalized model adaptation techniques. Additionally, the system incorporates strong validation techniques to protect against malicious model updates and allow scaled collaboration across edge-cloud infrastructures. All things considered, the sug- gested approach creates a collaborative intelligence paradigm for next-generation intelligent transportation systems that is safe, scalable, and reliable.

Related Work

Federated Learning (FL) was initially proposed by McMahan *et al.* [1], introducing the Federated Averaging (FedAvg) algorithm as a decentralized approach for collaborative model aggregation. Li et al. [2] developed the Federated Proximal (FedProx) optimization techniques, which stabilize training under non-IID data distributions to resolve the challenges imposed by statistical variation among distributed clients. Additionally, a thorough survey describing important open research topics in scalability, robustness, privacy preservation, or customization in federated systems was published by Kairouz et al. [3]. Subsequently, block chain-integrated FL frameworks were investigated to mitigate centralized trust dependencies and enhance transparency, security, and decentralized coordination. Kim *et al.* [4] and Wang *et al.* [5] integrated blockchain for secure aggregation and auditability. Secure aggregation and privacy-preserving mechanisms were further studied by Bonawitz *et al.* [6] and Geyer *et al.* [7]. Byzantine-resilient aggregation methods were introduced by Blanchar *et al.* [8], and hierarchical edge–cloud federated architectures were proposed by Liu *et al.* [9].

Table1: Comparison with Existing Work

Reference	Personalization	Block chain	Robustness	Multi-Cloud
[1]	No	No	No	No
[2]	Yes	No	No	No
[3]	Yes	No	No	No
[4]	No	Yes	Partial	No
[5]	No	Yes	Partial	No
[6]	No	No	Yes	No
[7]	No	No	Yes	No
[8]	No	No	Yes	No
[9]	No	No	Partial	Partial

Beyond these foundational studies, recent research has explored incentive-driven federated learning for participant reliability [11], reputation-based trust management models [12], asynchronous federated optimization strategies [13], meta-learning–based personalization approaches [14], and clustered federated learning for handling data heterogeneity [15]. Communication efficient gradient compression schemes were investigated in [16], while optimal client selection mechanisms were proposed in [17]. Secure multi-party computation techniques for privacy-preserving aggregation were studied in [18], and decentralized peer-to-peer federated learning architectures were developed in [19]. Furthermore, scalable block chain sharing mechanisms for distributed systems were analyzed in [20].

Despite these advancements, existing works do not simultaneously integrate personalized edge-level adaptation, proxy-based anomaly monitoring, and multi-cloud peer-to-peer aggregation within a unified block chain-enabled federated framework for autonomous vehicle ecosystems. The proposed approach addresses these limitations through secure smart- contract driven aggregation, decentralized trust management, scalability across cloud clusters, and adversarial robustness.

Research Gap and Problem Statement

Despite significant advancements in block chain-integrated architecture with federated learning, a number of basic issues still exist, especially in autonomous vehicle (AV) ecosystems. Many current solutions still rely on centralized cloud-based aggregation, as shown in Table2, which exposes them to single-point-of-failure concerns that cause scalability difficulties. Also, the present framework's capacity to manage heterogeneous and non-IID data distributions across various AV manufacturers and operational contexts is restricted by inadequate personalization tactics. Inadequate methods for monitoring and validating Byzantine risks, particularly poisoning models, make safety crucial. Additionally, frequent global updates lead to high communication overhead, which significantly reduces large-scale edge-cloud infrastructure operating efficiency. These drawbacks highlight the need for a block chain- enabled, decentralized, flexible, and robust federated learning architecture that facilitates safe multi-cloud orchestration, customized model adaptation, and robust adversarial defense mechanisms.

Table 2: Current Block chain-Enabled Federated System Drawback

No.	Challenges	Effects on AV Ecosystems
1	Centralized cloud aggregation bottlenecks	Introduces single-point-of-failure risks, increases latency, and limits scalability across geographically distributed autonomous vehicle clusters.
2	Limited personalization for heterogeneous AV manufacturers	Degrades model accuracy due to non-IID data distributions and varying sensor modalities across manufacturers and driving environ- ments.
3	Weak monitoring against model poisoning attacks	Reduces robustness against Byzantine, adversarial, and backdoor attacks, compromising system reliability and safety-critical decision-making.
4	High communication overhead	Increases bandwidth consumption and training latency, making large-scale deployment across edge–cloud infrastructures inefficient.

Problem Statement:

Developing a robust and fully decentralized federated learning framework for autonomous vehicle ecosystems is challenging due to heterogeneous data distributions, security threats, and large-scale deployment constraints. The key challenge lies in constructing a trust- independent collaborative learning architecture that overcomes centralized aggregation limitations while enabling secure model sharing, efficient communication, personalized adaptation, and strong defense against poisoning and Byzantine attacks across distributed edge-cloud infrastructures.

Proposed Block Chain-Enabled Personalized Federated Frame- work

The proposed block chain-enabled personalized federated learning (BPFL) paradigm in Figure 1. is intended to solve issues with robustness, scalability, security, or personalization in autonomous vehicle (AV) ecosystems. Four strongly connected layers make up the architecture: (i) Edge Learning Layer, (ii) Proxy Monitoring Layer, (iii) Block chain Trust Layer, and (iv) Multi-Cloud Aggregation Layer. The complete operational pipeline encompasses distributed model initialization, secure verification of local updates, decentralized aggregation of model parameters, and adaptive personalization of the learned models.

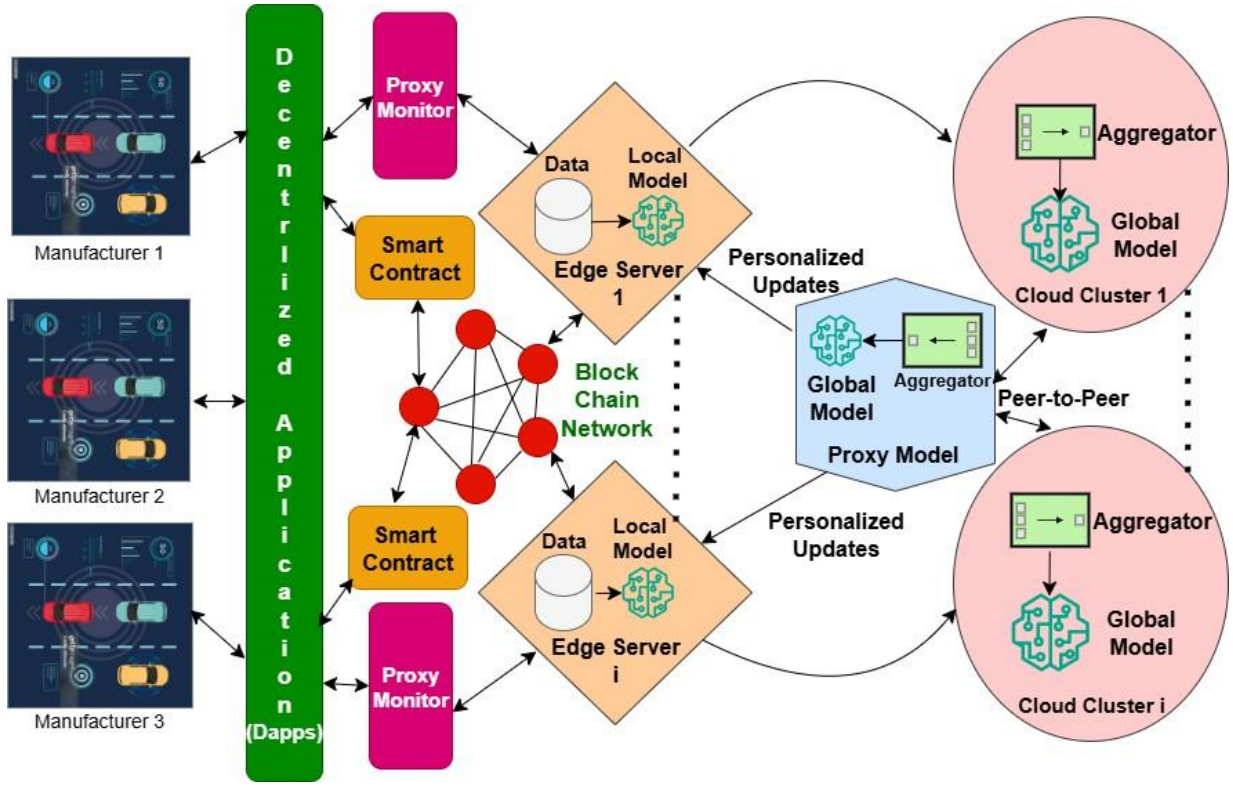

Figure1: Block chain-enabled Personalized Federated Learning (BPFL) framework

System Model and Notations

Let M= {1, 2. . . *M*} these to f AV manufacturers (clients) be denoted. Each manufacturer I possesses a private dataset D_i with sizen_j, such that:

$$D = {}_{i=1}^{M}\cup D_i,\ where\ D_i\ \cap\ D_j = \emptyset, i\ \neq j$$

The objective is to minimize the global empirical risk:

$$\min_w \mathrm{F(w)} = \sum_{i=1}^{M} \frac{n_i}{n} \mathrm{F_i(w)}$$

Where,

$$F_i(w) - {}^{1}/_{n_i} \sum_{(x,y)\in D_i} \ell(w; x, y)$$

Here, w represents model parameters and ℓ (·) is the loss function.

Edge Learning Layer

Each manufacturer deploys an edge server responsible for local model training. At the communication round t, the global model w^t is distributed to selected clients. Each client performs E local epochs using stochastic gradient descent (SGD):

$$w_i^{t+1} - w^t - \eta \nabla F_i(w^t)$$

Where:

(i) η is the learning rate,

(ii) $\nabla F_i(w^t)$, denotes local gradient.

To address non-IID heterogeneity, we introduce a regularized proximal objective:

$$F_i^{prox}(w) - F_i(w) + \frac{\mu}{2}\|w - w^t\|^2$$

Where μ controls drift from the global model.

Proxy Monitoring and Anomaly Detection

Before submitting updates to the block chain network, each local update undergoes validation through a proxy monitor module.

Let$\Delta w_i - w_i^{t+}{}_i^1 - w^t$.

An anomaly score is computed as:

$$S_i = \frac{\|\Delta w_i\|^2}{\sigma_t}$$

Where σ_t is the standard deviation of update norms in round t. If:

$$S_i > \tau$$

The update is flagged as malicious or poisoned and rejected.

Additionally, cosine similarity validation is performed:

$$\cos(\theta_i) - \frac{\Delta w_i . \dddot{\Delta w}}{\|\Delta w_i\| \|\dddot{\Delta w}\|}$$

Updates with negative similarity are discarded.

Block chain-Based Trust Management

Validated updates are recorded on a permission block chain network using Practical Byzantine Fault Tolerance (PBFT). Each update transaction includes:

(i) Hash of model weights: $H(w^{t+1})$

(ii) Manufacturer ID $_i$

(iii) Time stamp

(iv) Validation certificate

Smart contracts enforce the following:

(i) Update integrity verification

(ii) Participation tracking

(iii) Incentive scoring

(iv) Reputation management

The reputation score for the client i is updated as follows:

$$R_i^{t+1} = \beta R_i^t + (1-\beta)V_i^t$$

Where V_i^t represents validation outcome and β controls memory retention. Clients with low reputation are temporarily excluded from aggregation.

Decentralized Multi-Cloud Aggregation

Instead of a single centralized server, multiple cloud clusters perform peer-to-peer aggregation.

Weighted aggregation is computed as:

$$w^{t+1} - \sum_{i \in S_i} \frac{n_i R_i^l}{\sum_{j \in S_i} n_j R_j^l} w_i^{t+1}$$

where:

(i) S_t=set of validated clients

(ii) R^t=reputation weight

Clusters exchange global summaries via secure P2P synchronization to avoid single-point failure.

Personalized Model Adaptation

Due to manufacturer-specific driving environments and sensor configurations, strict global uniformity may degrade local performance. Therefore, a personalization layer refines the global model:

$$w_{i,personal}^{l+1} = \alpha \mathrm{w}^{l+1} + (1-\alpha)\mathrm{w}_\mathrm{i}^{l+1}$$

Where:

(i) $\alpha \in [0,1]$ controls personalization strength.

(ii) α=1 corresponds to a pure global model.

(iii) α=0 corresponds to a fully local model.

Adaptive α selection is computed using validation accuracy:

$$\boldsymbol{\alpha_i^* = arg\ max\ Acc_i(\alpha)}$$

Proposed Algorithm

Algorithm1 BPFL Algorithm

Require: Initialize with global parameters w^0, number of communication rounds T, set of participating clients C, learning rate η, initial reputation score $\{w_i^T\}$

Ensure: Personalized models for all clients w_i^T

For t= 1to T **do**

Select active clients $C_l \subseteq C$ based on availability and reputation scores. Broadcast the current global model w^{t-1} to selected clients.

For all client $i \in C_l$ in parallel **do**

Initialize local model $w_i^{t-1} \leftarrow w^{t-1}$

Train the model locally for E epochs using the dataset D_i

Compute local model

$$\Delta w_i^t = w_i^t - w^{t-1}$$

Apply gradient compression and secure encoding to obtain $\Delta\widetilde{w_i^t}$

Send compressed update to the proxy monitoring module.

End for

The proxy monitor evaluates updates using anomaly detection and Byzantine filtering.

Legitimate updates are accepted, and reputation scores $\{r_i^t\}$ are updated.

Hashes of validated updates are recorded on the block chain using smart contracts.

Compute normalized reputation-based weights.

Aggregates local models using decentralized reputation weighted aggregation.

Distribute the updated global model to edge servers.

Perform client-specific fine-tuning to obtain w_i^t

End for

return personalized models $\{w_i^t\}$

Communication Efficiency Optimization

To minimize communication bandwidth consumption, gradient compression techniques are incorporated into the training process. Specifically, top-k gradient scarification is employed to retain only the most significant gradient components, while quantization is applied to further compress model updates. In addition, only substantial weight variations are transmitted to the aggregator, thereby reducing redundant communication overhead. The compressed model update is expressed as

$$\Delta\widetilde{w_i} - Q_k(\Delta w_i),$$

Where Q_k (·) denotes the top-k operator that preserves gradient components with the highest magnitudes.

Computational Complexity

The computational challenge within the proposed BPFL architecture has been anticipated to get tested using three main elements. The complex nature of the local model training at each client is O(En_id), where d the size of the model, n_i is among the localized data with client i, where E represents the number of local rounds. O(Md) Operations are needed for the global aggregation round, which M=|C_t| is the number of clients that participated in a particular communication round. Additionally, taking in to account that the distributed validation process uses practical

Byzantine fault tolerance (PBFT), the communication complexity for parallel messages being transferred over N verification nodes is $O(N^2)$.

Experimental Setup

Multiple manufacturers working together, dispersed edge servers, and cloud-level aggregation clustersareallmodeledintheexperimentalconfiguration.Table3providesasummaryof the specific configuration options.

Table 3: Detailed Experimental Configuration

Parameter	Value
Number of Manufacturers (Clients)	5
Edge Servers (Regional Aggregators)	5
Cloud Clusters (Global Coordinators)	2
Total Simulated Vehicles	500
Dataset Type	Multimodal Simulated AV Sensor Data
Data Distribution	Non-IID across manufacturers
Model Architecture	Deep Neural Network (DNN)
Communication Rounds	100
Local Training Epochs (E)	5
Batch Size	32
Optimizer	Adam
Learning Rate	0.01
Personalization Factor (α)	0.6
Gradient Compression	Top-k Scarification (20%)
Block chain Type	Permission Network
Consensus Protocol	PBFT
Adversarial Clients Ratio	20% (Poisoning Simulation)
Evaluation Metrics	Accuracy, Communication Cost, Robustness Index

Results and Analysis

Using dynamically modifying aggregation weights based on validated client contributions and using edge-level fine-tuning, BPFL stabilizes gradient updates, decreases oscillations during training, and promotes global model generalization. As a result, the framework outperforms conventional central aggregator techniques in terms of optimization efficiency and asymptotic performance.

Performance Comparison

The comparative performance of different learning approaches is summarized in Table 4.

Table 4: Accuracy Comparison

Method	Accuracy (%)	Comm. Overhead(MB)
Centralized ML	89.3	1200
Vanilla FL	91.5	850
Block chain FL	92.8	900
Proposed BPFL	**94.2**	**690**

Accuracy vs Communication Rounds

The convergence dynamics of the proposed BPFL framework and traditional federated learning are compared in Figure 2. The finding shows that BPFL produces better steady-state reliability as it shows faster convergence in the early communication rounds. Reputation- weighted aggregation, which lessens the impact of in consistent or subpar client updates, and adaptive personalization techniques, which successfully handle non-IID data heterogeneity, are responsible for this improvement.

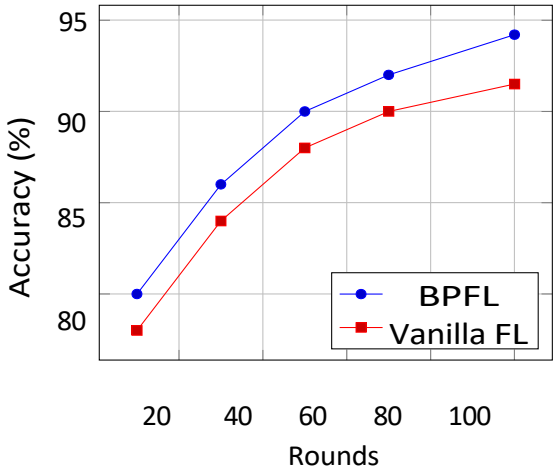

Figure2: Accuracy Improvement over rounds

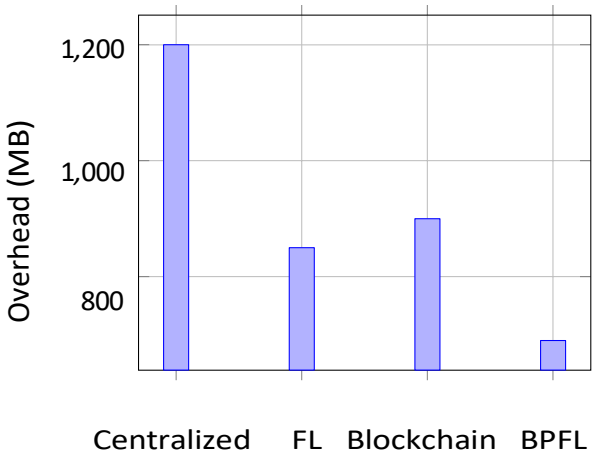

Figure3: Communication Overhead Comparison

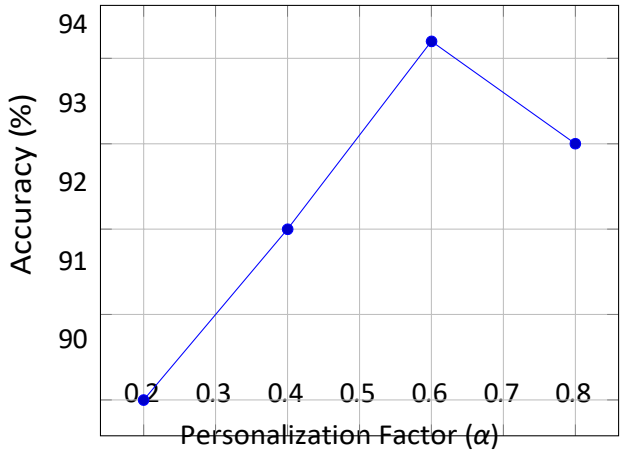

Figure4: Correlation between Personalization and Accuracy

Communication Overhead

The comparative communication costs between various collaboration learning models are shown in Figure 3. When compared to standard federated systems, the proposed BPFL architectures how a significant reduction in communication overhead. The merging of top-*k* gradients scarification and quantization-based compression, which significantly reduces the dimensionality and size of transmitted model updates, is the main method used to achieve this improvement. BPFL reduces superfluous data sharing during every communication cycle by transmitting exclusively encoded parameter differentials and large gradient components.

Correlation between Personalization and Accuracy

The link between the personalization coefficient (α) and the final model accuracy is shown in Figure 4.The finding shows that the best outcomes are obtained with an intermediate personalization weight (α = 0.6). Lower values α overly highlight global model parameters, restricting the framework's capacity to adapt to client-specific data distribution.

Conclusions

A block chain-enabled personalized federated learning (BPFL) architecture created especially for autonomous vehicle (AV) ecosystems functioning in hostile or heterogeneous contexts was presented in this paper. The proposed framework eliminates centralized trust assumptions while enhancing scalability and system robustness by combining smart contract-driven secure aggregation, proxy-assisted adversarial filtering, decentralized multi-cloud coordination, and edge-level personalization. By allowing distributed trust enforcement, transparent validation of client updates, and immutable recording of model transactions, the addition of the permission-based block chain component improves robustness against model poisoning and Byzantine behavior. According to experimental results, BPFL performs better in terms of global accuracy, convergence stability, and communication efficiency over traditional federated or centralized learning models. Local model performance under non-IID data distributions across several manufacturers is further enhanced by the adaptive customization technique. Together, the proposed design creates a collaborative learning infrastructure for next-generation intelligent transportation systems that is safe, scalable, and dependable.

References

[1] B. McMahan *et al.*, "Communication-efficient learning of deep networks from decentralized data," in *Proc. AISTATS*, 2017.

[2] T. Li *et al.*, "Federated optimization in heterogeneous networks," in *Proc. MLSys*, 2020.

[3] P. Kairouz *et al.*, "Advances and open problems in federated learning," *Foundations and Trends in Machine Learning*, vol. 14, no. 1–2, pp. 1–210, 2021.

[4] H. Kim, J. Park, M. Bennis, and S. Kim, "Blockchained on-device federated learning," *IEEE Communications Letters*, vol. 24, no. 6, pp. 1279–1283, 2020.

[5] Q. Wang *et al.*, "Blockchain-based federated learning for securedata sharing," *IEEE Network*, vol. 33, no. 5, pp. 72–79, 2019.

[6] K. Bonawitz *et al.*, "Practical secure aggregation for federated learning," in *Proc. ACM CCS*, 2017.

[7] R. Geyer, T. Klein, and M. Nabi, "Differentially private federated learning," in *Proc. NeurIPS Workshop*, 2017.

[8] P. Blanchard *et al.*, "Machine learning with adversaries: Byzantine tolerant gradient descent," in *Proc. NeurIPS*, 2017.

[9] Y. Liu *et al.*, "Client-edge-cloud hierarchical federated learning," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6076–6087, 2020.

[10] Y. Lu *et al.*, "Blockchain-enabled secure data sharing in vehicular networks," *IEEE Transactions on Vehicular Technology*, 2020.

[11] J. Kang *et al.*, "Incentive mechanism for reliable federated learning," *IEEE Internet of Things Journal*, 2019.

[12] X. Li *et al.*, "Reputation-based trustmanagement in blockchain-enabled FL," *IEEE Access*, 2020.

[13] H. Xie *et al.*, "Asynchronous federated optimization," *IEEE Transactions on Wireless Communications*, 2020.

[14] A. Fallah, A. Mokhtari, and A. Ozdaglar, "Personalized federated learning with meta-learning," in *Proc. NeurIPS*, 2020.

[15] F. Sattler *et al.*, "Clustered federated learning," *IEEE Transactions on Neural Networks and Learning Systems*, 2021.

[16] S. Caldas *et al.*, "Expanding the reach of federated learning by reducing communication," in *Proc. NeurIPS Workshop*, 2018.

[17] Y. Chen *et al.*, "Optimal client selection for federated learning," *IEEE Transactions on Communications*, 2021.

[18] J.So*etal.*,"Securemulti-partycomputationforfederatedlearning,"in*Proc.IEEE Symposium on Security and Privacy*, 2022.

[19] A.Lalitha*etal.*,"Peer-to-peerfederatedlearningongraphs,"*IEEETransactionson Signal Processing*, 2019.

[20] M.Kim*etal.*,"Scalableblockchainshardingforfederatedsystems,"*IEEEAccess*,2021.