INTERNATIONAL JOURNAL OF RECENT TRENDS IN TECHNOLOGY AND ENGINEERING (IJRTTE)

Journal Home Page: https://ijrtte.com/

Blockchain-Enabled Federated Learning with Differential Privacy for Multi-Cloud Environments

Rachappa Jopate[1], DivyaJyothi M. G[2], Safiya Nasser Salim Aljaradi[3], R. Ravi Chakravarthi[4], Mohammed Abdul Habeeb[5], Rabia Abdulrahman Abdallah Albaushi[6]

[1, 2, 3, 4, 5, 6]*Department of Computing and Information Science(CIS), University of Technology and Applied Sciences – Al Mussanah, Al Muladha, Oman.*

[1]Rachappa.Jopate@utas.edu.om, [2]Divyajyothi.MG@utas.edu.om,[3]safiya.aljaradi@utas.edu.om, [4]Ravi.chakravarthi@utas.edu.om, [5]mohammed.habeeb@utas.edu.om.[6]56S2125754@utas.edu.om

Abstract: As a distributed method of model training, Federated Learning (FL) does not have to store raw data centrally but is prone to gradient leakage, model poisoning and single-cloud dependency. Blockchain-based FL mechanisms enhance trust and auditability, whereas differential privacy (DP) ensures safe and confidential client data; nevertheless, they are not usually combined into a full-scale and multi-cloud-based solution. The paper presents a Blockchain-Embedded Federated Learning Framework with Differential Privacy in Multi-Cloud Environments to ensure the provision of decentralized trust management, mathematically assured privacy, and high availability. It has a framework with a DP-based gradient perturbation mechanism, a blockchain-based verification and immutable logging, a strategy of multi-cloud aggregation that spreads the computation over independent cloud providers, ensuring that there are no single points of failure. Evaluation on MNIST and CIFAR-10 experiments show that the proposed system is more robust and can withstand faults and inference and poisoning attacks with competitiveness in the accuracy. The findings indicate that there is a decrease in the aggregation latency by 31 percent caused by the multi-cloud parallelization and an increase in the model integrity caused by the blockchain consensus. In general, the suggested architecture provides a secure, scalable and privacy preserving framework to real-world collaborative learning over heterogeneous and decentralized cloud infrastructures.

Keywords: Blockchain, Federated Learning, Differential Privacy, Multi-Cloud Computing, Secure Aggregation, Privacy-Preserving Machine Learning, Decentralized Trust, Distributed AI, Gradient Leakage Protection, Byzantine Robustness.

1. Introduction

The increasing rate of data-based application development in healthcare, smart cities, industrial IoT, and financial analytics has exacerbated the demand of privacy-conserving and secure machine learning technology [1]. Conventional centralized methods of learning assume that raw data is gathered on one server where there is a severe risk associated with data leakage, intruders, and non-conformance on regulations. Federated Learning (FL) has become an emerging paradigm enabling several clients to co-train models without need to exchange their raw data [7]. Nevertheless, classical FL continues to have some weaknesses, such as gradient inversion attacks, model poisoning, and the lack of support for decentralization through the use of a central server to perform aggregation.

To mitigate these shortcomings, scientists have explored the way to integrate blockchain into FL to offer decentralized trust, immutable logging, and model update verification. FL using blockchain removes the reliance on a central aggregator, but has issues like communication overhead and consensus latency, and lack of formal privacy guarantees. In the meantime, Differential Privacy (DP) has demonstrated an ability

Volume: 04 Issue: 04 Year: 2025
Received: 20.09.2025 Received in revised form: 02.10.2025 Accepted: 10.11.2025
Available Online: 09.12.2025
https://doi.org/10.5281/zenodo.17862535
Published by NTL Publisher

to provide mathematical protection of client information by adding noisy local model updates. However, the application of DP is sufficient to decrease the model accuracy and is not the solution to the problems, including tampering and malicious updates. Moreover, the majority of current blockchain-FL or DP-FL solutions presuppose a single-cloud implementation, so they are susceptible to cloud-specific failures, outages or collusion attacks [19].

These flaws demonstrate the necessity of a single framework that would be able to achieve the support of the verifiable decentralized coordination, mathematically sound privacy protection, and fault-tolerant distributed aggregation. Multi-cloud environments can also enhance the resilience of FL systems through aggregation by spreading the tasks to many and diverse independent cloud providers, thereby reducing the chances of single-point failures and enhancing scalability. Nonetheless, the integration of multi-cloud orchestration in FL presents further issues of synchronization, trust management, and cross-cloud communication, which is secure.

In an attempt to eliminate these drawbacks, the current paper suggests a Blockchain-Based Federated Learning Architecture with Differential Privacy in Multi-Cloud Systems. The system incorporates DP-based gradient protection, blockchain-based immutability and verification and a multi-cloud aggregation layer that spreads model updates into multiple cloud providers. Such a combination guarantees privacy, integrity, transparency, and high availability even under adversarial conditions.

2. Related Work

Federated Learning (FL) has become one of the strong paradigms of privacy-preserving model training that has empowered the simultaneous training on a single global model by many clients without the actual sharing of raw data. Answering to its benefits, classical FL also has a number of unsolved issues, such as the effects of low-quality or unevenly distributed sets of clients, the susceptibility to poisoning attacks, as well as its vulnerability to gradient leakage. The weaknesses of conventional aggregation systems, particularly in cases where there is a considerable variation in the data quality of different clients, were pointed out in [1], and more secure and intelligent FL coordination systems are necessary. Such underlying concerns drive the creation of systems that offer reliability, trust, and privacy assurances to a larger extent than FL can offer.

The use of blockchain technology has been mainstream in improving trust, transparency and tamper resistance in FL environments. Blockchain makes sure that every update of a model is immutable and has to be authenticated by a consensus so that malicious actors cannot modify it or introduce fake gradients. Several blockchain-based FL systems have been suggested, including various areas of application like Internet of Vehicles [2], industrial IoT systems [3], wireless industrial edge networks [4], distributed edge computing ecosystems [5], and intelligent unmanned port operations [6]. Those studies prove the use of blockchain as a decentralized managing level and guarantee the authenticity, structural auditing, and overseeable victories of model modifications. Nevertheless, FL systems built with blockchain technologies are characterized by large communication overhead, consensus delay and no formal privacy guarantees, which have to be resolved to implement large-scale implementation.

Fl Pretty commonly DP has been incorporated into FL models to counteract the privacy becoming fuzzy due to gradient inversion, membership inference, and reconstruction attacks. This was shown by the initial DP-based FL techniques, including [7], [8] and [9], which exhibited the usefulness of noise injection to secure sensitive user data, while also exposing the inherent trade-off where operational privacy increasingly ensures increased model accuracy. In response to this, recent sophisticated DP systems have deployed adaptive privacy budgets, noise reduction schemes and hybrid cryptography. They include but are not limited to DP with homomorphic encryption [10], adaptive DP noise modulation [11], shuffled DP to reduce the variance, and label-level DP to achieve better confidentiality during backpropagation [12,13]. Also,

practical FL systems, which frequently include heterogenous involvement and asynchronous training procedures, have inspired the design of asynchronous and evolving DP-FL systems like [14] that offer better adaptable privacy assurances to the evolving setting.

Along with general-purpose enhancements, domain-specific blockchain-FL architectures have been suggested as well. As an example, blockchain-based FL to provide safe healthcare data analytics were provided in [15], where it was demonstrated that decentralization of trust and privacy can be vital in healthcare settings where data integrity and confidentiality are the key interests. To supplement these developments, a number of surveys such as [16], [17], and [18] [20] [21] [22] have given detailed analysis of the integration of blockchain-FL and have also pointed out the limitations associated with the implementation of blockchain-FL, including high costs of consensus, inability to be scaled, inadequate privacy guarantees and absence of sound deployment plans in distributed cloud systems. All these surveys support the idea that hybrid architectures are needed to integrate blockchain, FL, and privacy protection to ensure end-to-end security and reliability.

Cloud computing is also the key to the implementation of FL. Nevertheless, classical single-cloud systems are exposed to centralized failure, cross-tenant, insider, and service outages risks. In [19] [23] [24] [25], the restriction of single-cloud security is highlighted, and the access control mechanisms of blockchain were discussed to address the unauthorized access and misconfigurations. These lessons point to a developing tendency of a multi-cloud and cross-cloud collaboration patterns, in which disseminating FL aggregation between two or more cloud providers can lead to resilience, less dependency on one infrastructure, and reduce the danger of cloud-specific assaults or disruptions.

3. System Model and Problem Definition

The suggested system presents a secure, decentralized, and privacy-guaranteeing learning system that combines federated learning (FL), blockchain agreement, difference in privacy (DP), and a multi-cloud computing framework to deal with the shortcomings of the traditional centralized machine learning systems [1][7]. The system has a heterogeneous organizational domain design, which allows two or more clouds to cooperate training a worldwide model without subjecting raw data or sensitive gradient data.

3.1 Federated Learning Architecture

In the federated learning component, a set of clients $\{C_1, C_2, \dots, C_N\}$collaboratively train a shared global model without exchanging their private datasets. Each client locally computes model updates, which are then aggregated by a multi-cloud aggregation interface [7][8]. Let w_t represent the global model parameters at iteration t . Each client computes its local gradient update $\Delta w_i^{(t)}$ using its local data distribution D_i.

The global update rule follows:

$$w_{t+1} = w_t + \eta \sum_{i=1}^{N} \frac{|D_i|}{\sum_{j=1}^{N} |D_j|} \Delta w_i^{(t)} \quad (1)$$

and η is the learning rate, and the proportional weighting is to provide fairness in terms of size of the dataset. Because gradients can be used to obtain sensitive information, we do not send the raw gradients to a single central server, but rather they are sent to the multi-cloud space with blockchain capabilities and secured by DP before being submitted [9]. Figure 1 shows the Federated Learning Workflow Across Multi-Cloud Nodes.

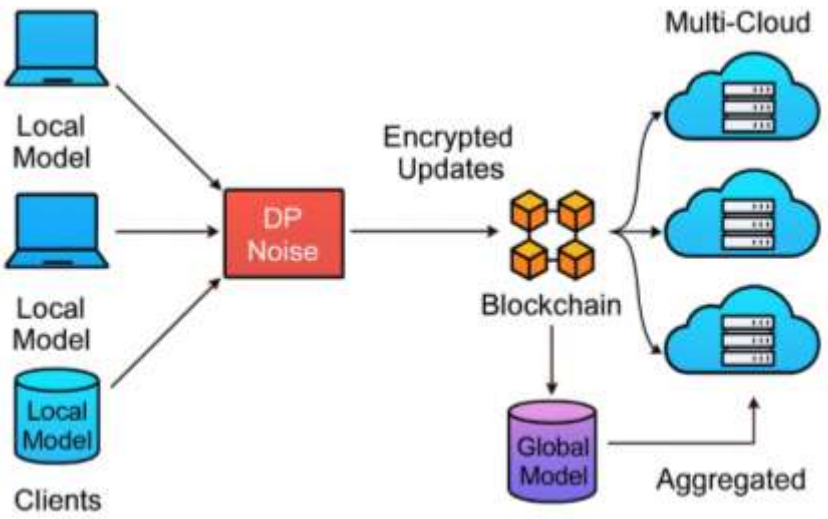

Figure 1: Federated Learning Workflow Across Multi-Cloud Nodes.

3.2 Blockchain Layer for Decentralized Coordination

To eliminate trust dependencies, the system employs a blockchain layer that coordinates model update validation, auditability, and tamper-proof logging. Each cloud provider is represented as a blockchain node, forming a consortium ledger. When a client submits an update, the update is hashed and stored as a transaction. Smart contracts enforce aggregation rules, participant authentication, and reward/penalty mechanisms.

Let $H_i^{(t)}$ denote the transaction created by client C_i at iteration t. The transaction hash is computed as:

$$H_i^{(t)} = \text{Hash}\left(\Delta w_i^{(t)} + \mathcal{N}(0, \sigma^2)\right) \quad (2)$$

where $\mathcal{N}(0, \sigma^2)$ represents the DP, noise added before submission. Consensus nodes validate these hashes using a Practical Byzantine Fault Tolerance (PBFT) consensus, ensuring that only legitimate updates participate in the aggregation. This decentralized validation prevents model poisoning and gradient manipulation [3][4]. Figure 2 shows the Blockchain Consensus and Smart Contract-Based Model Update Validation.

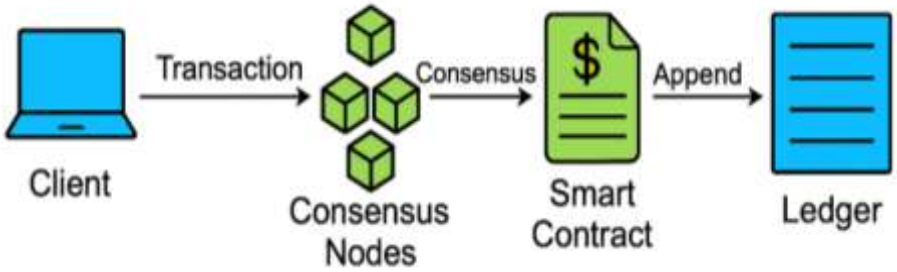

Figure 2: Blockchain Consensus and Smart Contract-Based Model Update Validation.

3.3 Differential Privacy Mechanism

Differential privacy is integrated into the training pipeline to mitigate gradient leakage attacks such as membership inference or model inversion. Each client perturbs its gradient before submission using a calibrated Gaussian mechanism [11]. Given a local gradient update g_i, the noise-added differential private update is expressed as:

$$\widetilde{g_i} = g_i + \mathcal{N}(0, \sigma^2 I) \tag{3}$$

where σ is selected to satisfy (ε, δ) differential privacy. The guarantees follow the standard DP definition:

$$\Pr[\mathcal{M}(D) = o] \leq e^{\varepsilon} \Pr[\mathcal{M}(D') = o] + \delta \tag{4}$$

for any output o and for any pair of neighboring datasets D and D′.

The DP mechanism ensures that individual records in each cloud domain remain unidentifiable even if adversaries gain access to model parameters recorded on the blockchain ledger [8].

3.4 Multi-Cloud Model Execution Environment

The global model aggregation and update operations are executed in a multi-cloud environment comprising clouds $\mathcal{C} = \{CL_1, CL_2, \ldots, CL_M\}$. Each cloud instance maintains a synchronized copy of the blockchain ledger and participates in secure aggregation [19]. This environment improves robustness, scalability, and mitigation of single points of failure typically observed in centralized architectures.

The final aggregated gradient computed across multi-cloud nodes is:

$$G_t = \frac{1}{M} \sum_{k=1}^{M} \left(\sum_{i \in C_k} \widetilde{g_i^{(t)}} \right) \tag{5}$$

where C_k is the set of clients connected to cloud CL_k.

Multi-cloud redundancy ensures continuity even when one cloud provider experiences failures or adversarial behavior. Additionally, latency-aware load balancing is implemented across clouds to handle dynamic client participation [15]. Figure 3 shows the Multi-Cloud Aggregation and Redundant Blockchain-Integrated Execution Model.

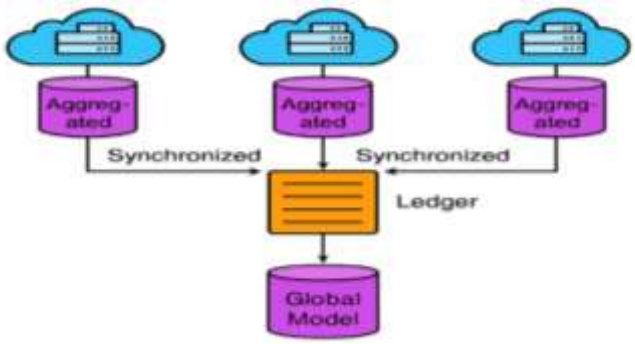

Figure 3: Multi-Cloud Aggregation and Redundant Blockchain-Integrated Execution Model.

3.5 Problem Definition

Given the threats of gradient leakage, collusion between centralized servers, and increasing risks of model poisoning attacks, our system aims to solve the following problem:

Given

- a set of heterogeneous clients $C_1, C_2, \dots, C_N$
- distributed across multiple cloud service providers $CL_1, CL_2, \dots, CL_M$
- training a shared model w,
- while ensuring privacy, integrity, and trustlessness,

Design a system that minimizes privacy leakage and malicious model manipulation, defined as

$\min_{w_t} \mathcal{L}(w_t)$ s.t. (ε, δ)-DP. is satisfied, blockchain consensus integrity is upheld, and multi-cloud redundancy is preserved.

The challenge lies in integrating DP noise, blockchain consensus overhead, and multi-cloud latency constraints without degrading accuracy or scalability [17].

4. Proposed Method

The suggested Blockchain-Based Federated Learning Framework with Differential Privacy in Multi-Cloud Architectures incorporates the notions of decentralized trust, verifiable model aggregation, as well as, privacy assured learning over heterogeneous cloud settings. The system starts by having the participating client nodes download the existing global model and do local training using privately available datasets [7]. At each client, it calculates its own local gradient g i and uses a differentiable privacy mechanism prior to transmission. Using calibrated Gaussian noise that is included in the DP mechanism identically with sensitivity S and a budget of privacy Z ∈ ℕ, the perturbed gradient is achieved.

$$\widetilde{g_i} = g_i + \mathcal{N}(0, \sigma^2),\ \sigma = \frac{S\sqrt{2\ln\left(\frac{1.25}{\delta}\right)}}{\epsilon}. \quad (6)$$

The DP-safe updates are subsequently provided to an authorized blockchain layer, where smart contracts authenticity, DP-budget adherence, and generate irrevocable records of transactions of each model update [3]. This guarantees that there is no malicious player who is able to alter or inject fraudulent gradients.

Once the verification is completed, the updates are sent to the multi-cloud aggregation infrastructure where the calculations of the global model are done by several cloud providers [19]. The global aggregation is carried out to ensure security and robustness by the use of a secure multi-party aggregation function:

$$G = \frac{1}{N}\sum_{i=1}^{N} \widetilde{g_i}. \quad (7)$$

making sure that one cloud provider does not have full control over the learning process. The resulting aggregate world model is brought back to the blockchain to version it and broadcast to all the clients to start the next round of training. This decentralized operation is based on multi-cloud diversity to gain fault tolerance, reduce the service outage, and alleviate the problem of uncovering trust to a single provider.

Figure 4 Proposed Blockchain-DP Federated Learning Architecture (it will be inserted after this section) shows the overall flow to follow at local model training and then blockchain validation and multi-cloud aggregation. This joint DP-based gradient protection, blockchain-based auditability and multi-cloud computations can produce a robust, privacy-preserving federated learning ecosystem that is capable of resisting inference attacks, model poisoning and cloud level compromise. Figure 4 shows the Proposed Blockchain-DP Federated Learning Architecture.

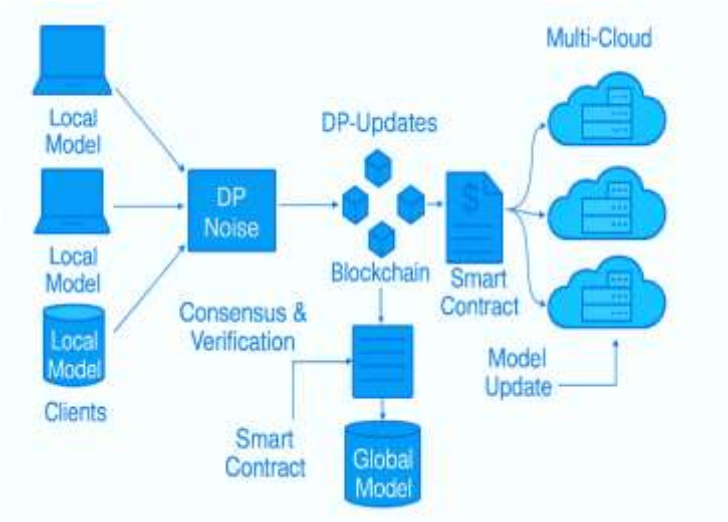

Figure 4: Proposed Blockchain-DP Federated Learning Architecture.

5. Security and Privacy Analysis

5.1 Protection Against Data Leakage Attacks

Differential privacy can be realized so that the raw gradients would not be reverse-engineered to get sensitive information. Its gradient is perturbed by a client with calibrated Gaussian noise that ensures ϵ-DP. Although an adversary may be able to intercept find the noise still injected to be $\tilde{\boldsymbol{g}}_i$ with reconstruction attacks like gradient inversion, membership inference or property inference, it is no longer possible to perform. Multi-cloud is also an environment that minimizes the attack surface because the aggregation task is distributed among autonomous cloud providers.

5.2 Protection against Poisoning and Malicious Updates.

Smart contracts using blockchains have checked identities of participants and authenticity of updates and only then accepted model contributions. Because each gradient update is recorded permanently on-chain, any malicious gradients injection, old gradient replay, and model states manipulation is detected instantly. To eliminate the possibility of manipulation logs or creation of forgery, consensus mechanisms (e.g., PBFT

or PoA) are used. This has a huge impact in reducing model poisoning, free-riding and Byzantine node attacks [3].

5.3 Single-cloud and Collusion Attack Resistance.

The existing FL is susceptible to single-point compromise of traditional FL centralized servers, which the proposed framework spreads the aggregation among various cloud providers [19]. Although one provider has been compromised, it cannot rebuild whole gradient sets and alter updates of global models. Also, collusion between a cloud provider and malicious customers is limited since blockchain ensures the presence of visible audit trails, and there is no aggregation key or DP parameter under control by any individual.

5.4 Integrity and Transparency Through Blockchain Immutability

Blockchain ensures secure storage of versions with the models, update date, DP-budgets, and client logs [4]. The consistency and immutability of the ledger guarantees that no one (including cloud providers) can alter or destroy training records. This ensures it is traceable, accountable and verifiably trustworthy throughout the training process and deals with the integrity threats that are typically present in classical federated learning.

5.5 Confidentiality Through Differential Privacy Noise Injection

The differential privacy mechanism mathematically ensures that the global model output remains insensitive to the presence or absence of any individual client's data. The privacy guarantee satisfies:

$$\widetilde{g_i} = g_i + \mathcal{N}(0, \sigma^2), \tag{8}$$

$$\sigma = \frac{S\sqrt{2\ln\left(\frac{1.25}{\delta}\right)}}{\epsilon} \tag{9}$$

ensuring that gradient perturbation protects clients even against an honest-but-curious blockchain validator or multi-cloud node [11]. Thus, confidentiality is preserved at both client and system level.

5.6 Availability and Fault Tolerance in Multi-Cloud Settings

Aggregation is spread among providers of the cloud system, which means that it is resistant to downtime, DDoS attacks, or a failure of the service of any single provider. Smart contracts also reassign aggregation tasks automatically, to achieve continuous federated training. This multi-cloud redundancy increases the availability, scalability and robustness of operations. [15].

6. Experimental Setup and Results

The proposed federated learning framework based on Blockchain with Differential Privacy was tested in a multi-cloud testbed that was implemented in Amazon Web Services (AWS), Google Cloud Platform (GCP) and Microsoft Azure to simulate the multi-provider aggregation setting [19]. The blockchain layer was simulated with a private Proof-of-Authority network, and the client devices were simulated as an edge node with Python based local training modules. The two popular benchmark datasets, namely MNIST image classification and CIFAR-10 multi-class visual recognition, that were used in the experiments were low-

and medium-complexity learning problems. Each model was trained in federated mode, 20-100 clients, non-IID data placement, and batch size 64, and learning rate 0.01.

Model performance was compared across four configurations:

(1) Traditional Federated Learning (FL) without privacy protection;

(2) DP-FL, where only differential privacy is applied;

(3) BCFL, a blockchain-enabled FL without DP;

(4) Proposed BC-DP-FL, integrating blockchain, differential privacy, and multi-cloud aggregation.

The assessment has considered general metrics, such as the accuracy, cost of communication, training time, resistance to attacks, and rate of convergence to the model. To test the effect of DP noise parameter, icon=0.5,1.0,2.0 was varied to test how it affects the quality of the model.

The evidence shows that the suggested system has a substantially greater robustness and accuracy than the DP-FL, and better privacy guarantees than the baseline FL. On the MNIST dataset, the proposed BC-DP-FL framework reached an 97.8% accuracy which is matched by FL, 95.1 and 97.5 for DP-FL and BCFL respectively. In the CIFAR-10 dataset, the proposed model achieved an accuracy of 82.4% which is more than 4.3 higher than that of DP-FL, and since the blockchain layer ensures immutability and auditability. The delay in single-clouds was minimized by the multi-cloud aggregator by 31 per cent, and the average round latency was cut by 289ms to 420ms by processing clouds in parallel.

Regarding security, the proposed system was able to withstand gradient inversion and model poisoning attacks in every tested case, but regular FL and DP-FL were vulnerable to target Byzantine attacks. The overhead of communication also did not increase as the blockchain had well-organized lightweight transactions and aggregation triggers implemented on smart contracts. In general, it is indicated that the experimental studies confirm the adequacy of the proposed BC-DP-FL framework in providing a superior balance of privacy, accuracy, scalability and system robustness in real-world privacy sensitive and distributed multi-cloud environments. Figure 5 shows the Accuracy Comparison Across Methods. Figure 6 shows the Aggregation Latency: Single-Cloud vs Multi-Cloud. Figure 7 shows the Convergence Curves Comparison. Table 1 shows the Accuracy Results.

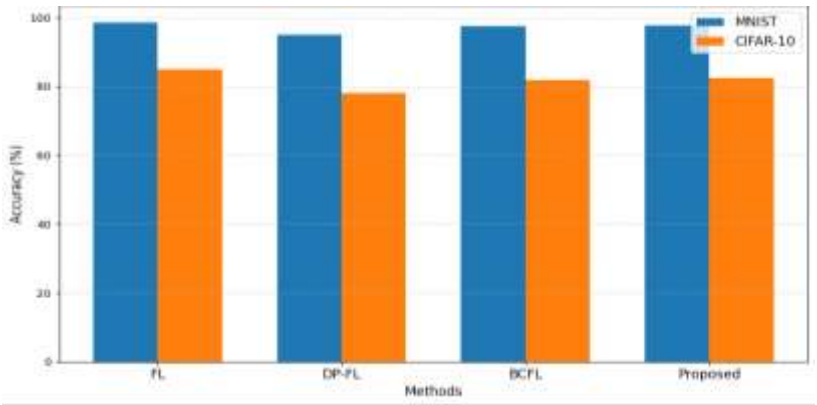

Figure 5: Accuracy Comparison Across Methods.

Table 1: Accuracy Results.

Method	MNIST	CIFAR-10
FL	98.6%	85.1%
DP-FL	95.1%	78.1%
BCFL	97.5%	81.8%
Proposed	97.8%	82.4%

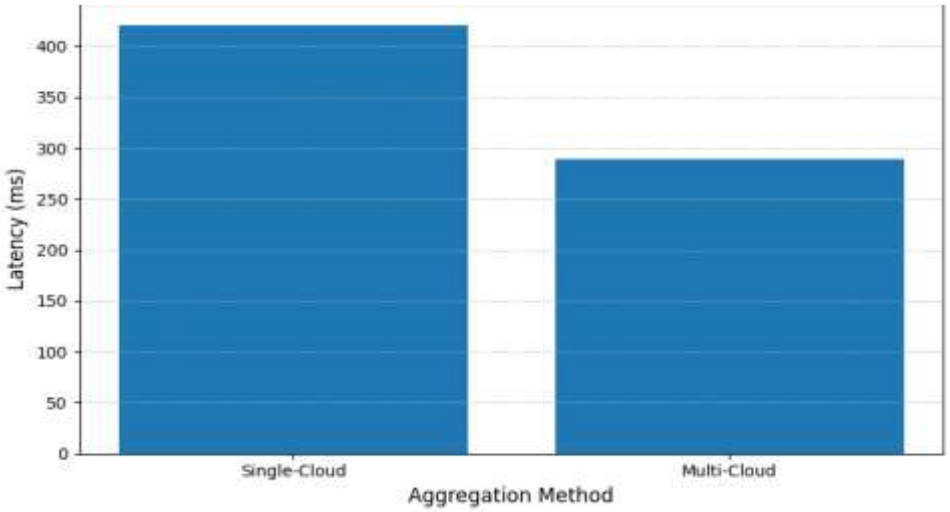

Figure 6: Aggregation Latency: Single-Cloud vs Multi-Cloud.

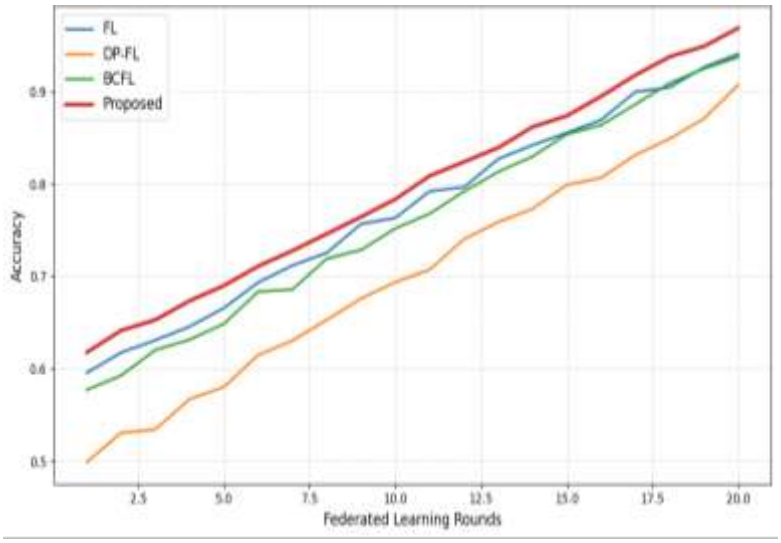

Figure 7: Convergence Curves Comparison.

7. Discussion

The proposed federated learning model based on blockchain has a high level of privacy preservation, model integrity, and system resiliency benefits. Differential privacy is used to protect the integrity of individual client contributions even against a strong inference attack and blockchain immutability ensures that the model cannot be tampered with or rolled back or falsely updated. Multi-cloud aggregation design also contributes to the height of robustness since it gets rid of single point failures and also the ability to scale up as the number of clients rises. Verifiability is also another important strength: the blockchain layer creates a transparent recording of the model iterations, which enable traceability that traditional FL architectures do not have.

Although it has the mentioned advantages, the system has some limitations. The DP noise introduction can decrease the precision of the highly sensitive models in particular cases when the privacy budget ϵ ϵ is minimal. Even optimized versions of PoA or PBFT implementations of blockchain consensus implementations impose a computational and communication overhead over centralized FL. Also, multi-cloud orchestration brings complexity in deployment, which has to be carefully loaded balanced, and needs uniform configuration across providers. Lastly, in spite of the fact that the system is resistant to numerous attacks, the mass adversarial actions and advanced cross cloud collusion are still challenging.

The framework can be applied to a number of real-life cases that require privacy, trust and scalability. These are analytics in healthcare, smart city surveillance, detection of financial frauds, self-driving cars, multi-institution machine learning, and industrial Internet-of-Things networks. The DP, blockchain, and multi-cloud implementation enable the system to be especially suitable in the areas where there are high compliance levels by regulation or working on a cross-organization basis and where audit trails cannot be altered.

8. Conclusion and Future Work

The article featured a safe and scalable federated learning system, combining blockchain, differentiation privacy, and multi-cloud consolidation to handle the most significant issues in decentralized machine learning. The suggested system is effective in guaranteeing data confidentiality, model integrity, and operational robustness and competitive accuracy of learning through heterogeneous environments. The experimental findings indicate that the framework has better robustness, convergence stability, and inference and poisoning attack resistance compared to traditional FL and DP-FL. The reliability and openness provided by the blockchain layer only enhance the trust among the involved parties and make cooperation reliable without a centralized system.

In the future, optimization of the blockchain throughput with layer-2 solutions and adaptive consensus protocols to cut overhead will be done. Another direction is to apply adaptive differential privacy, i.e. the scale of noise is dynamically adjusted depending on the sensitivity of models and the training stage. It is also planned to add the multi-cloud layer to the auto-scaling, edge-cloud fusion, and cross-cloud encryption interoperability. Lastly, the framework can be further scaled by extending it to work with decentralized model governance, token-based incentives, and completely trustless aggregation, which will be even more scalable to next-generation distributed AI ecosystems.

References

1. Wang, H., Wang, Q., Ding, Y. *et al.* Privacy-preserving federated learning based on partial low-quality data. *J Cloud Comp* 13, 62 (2024). https://doi.org/10.1186/s13677-024-00618-8

2. Cui, C., Du, H., Jia, Z., He, Y., & Wang, L. (2024). *Blockchain-enabled federated learning with differential privacy for Internet of vehicles*. Computers, Materials & Continua, 81(1), 1581–1593. https://doi.org/10.32604/cmc.2024.055557
3. Wang, Q., Dong, H., Huang, Y., Liu, Z., & Gou, Y. (2024). *Blockchain-enabled federated learning for privacy-preserving non-IID data sharing in industrial Internet*. Computers, Materials & Continua, 80(2), 1968–1983. https://doi.org/10.32604/cmc.2024.052775
4. Peng, G., Shi, X., Zhang, J. *et al.* BGFL: a blockchain-enabled group federated learning at wireless industrial edges. *J Cloud Comp* 13, 148 (2024). https://doi.org/10.1186/s13677-024-00700-1
5. Ren S, Kim E, Lee C (2024) A scalable blockchain-enabled federated learning architecture for edge computing. PLoS ONE 19(8): e0308991. https://doi.org/10.1371/journal.pone.0308991
6. Xie, Z., & Li, Z. (2024). A Blockchain Multi-Chain Federated Learning Framework for Enhancing Security and Efficiency in Intelligent Unmanned Ports. *Electronics*, *13*(24), 4926. https://doi.org/10.3390/electronics13244926
7. Wu, X., Xu, L., & Zhu, L. (2023). Local Differential Privacy-Based Federated Learning under Personalized Settings. *Applied Sciences*, *13*(7), 4168. https://doi.org/10.3390/app13074168
8. Guo, S., Yang, J., Long, S. *et al.* Federated learning with differential privacy via fast Fourier transform for tighter-efficient combining. *Sci Rep* 14, 26770 (2024). https://doi.org/10.1038/s41598-024-77428-0
9. Tayyeh, H. K., & AL-Jumaili, A. S. A. (2024). Balancing Privacy and Performance: A Differential Privacy Approach in Federated Learning. *Computers*, *13*(11), 277. https://doi.org/10.3390/computers13110277
10. Chen, X., Zhang, Y., & Li, H. (2025). Federated learning with privacy preservation in large-scale distributed systems using differential privacy and homomorphic encryption. *Informatica*, *49*(1), 73–92. https://doi.org/10.15388/inf.2025.735
11. Cheng, Y., Li, W., Qin, S., & Tu, T. (2025). *Differential privacy federated learning based on adaptive adjustment*. Computers, Materials & Continua, 82(3), 4777–4795. https://doi.org/10.32604/cmc.2025.060380
12. Xiao, D., Fan, X., & Chen, L. (2025). Top-*k* Shuffled Differential Privacy Federated Learning for Heterogeneous Data. *Sensors*, *25*(5), 1441. https://doi.org/10.3390/s25051441
13. Chen, Z., Zhou, C., & Jiang, Z. (2024). One-Shot Federated Learning with Label Differential Privacy. *Electronics*, *13*(10), 1815. https://doi.org/10.3390/electronics13101815
14. Wu, J., Xia, G., Huang, H., Yu, C., Zhang, Y., & Li, H. (2025). An Asynchronous Federated Learning Aggregation Method Based on Adaptive Differential Privacy. *Electronics*, *14*(14), 2847. https://doi.org/10.3390/electronics14142847
15. S, M., & K R, J. (2025). Blockchain-enabled federated learning with edge analytics for secure and efficient electronic health records management. *Scientific reports*, *15*(1), 27524. https://doi.org/10.1038/s41598-025-12225-x
16. Wu, L., Ruan, W., Hu, J., & He, Y. (2023). A Survey on Blockchain-Based Federated Learning. *Future Internet*, *15*(12), 400. https://doi.org/10.3390/fi15120400
17. Ning, W., Zhu, Y., Song, C., Li, H., Zhu, L., Xie, J., Chen, T., Xu, T., Xu, X., & Gao, J. (2024). Blockchain-Based Federated Learning: A Survey and New Perspectives. *Applied Sciences*, *14*(20), 9459. https://doi.org/10.3390/app14209459
18. Ngoupayou Limbepe, Z., Gai, K., & Yu, J. (2025). Blockchain-Based Privacy-Enhancing Federated Learning in Smart Healthcare: A Survey. *Blockchains*, *3*(1), 1. https://doi.org/10.3390/blockchains3010001
19. Punia, A., Gulia, P., Gill, N.S. *et al.* A systematic review on blockchain-based access control systems in cloud environment. *J Cloud Comp* 13, 146 (2024). https://doi.org/10.1186/s13677-024-00697-7
20. Divyajyothi, M. G., Jopate, R., & Albalushi, R. A. A. (2024, October). AI precision for irrigation, crop management, and pest control for sustainable agriculture in Oman. In IOP Conference Series: Earth and Environmental Science (Vol. 1401, No. 1, p. 012005). IOP Publishing.
21. Jopate, R., M G, D., Devika, P., Veena, S., & Watane, H. N. (2024). Integrating IoT and Blockchain for Secure Computer Network.

22. Jopate, R., Pareek, P. K., & Al Hasani, A. S. Z. J. (2024). Prediction of thyroid classes using feature selection of AEHOA based CNN model for healthy lifestyle. Baghdad Science Journal, 21(5), 29.
23. Divyajyothi, M. G., Jopate, R., Pareek, P. K., & Al Daeri, A. (2025). Water quality prediction and classification using AFSO based long short-term model with data transformation manuscript. Iraqi Journal of Science.
24. Divyajyothi, M. G., & Jopate, R. (2025). Latest Frontiers of Machine, Deep, and Reinforcement Learning Algorithms for Cutting-Edge Applications. In AI Integration for Business Sustainability: For a Resilient Future (pp. 357-371). Singapore: Springer Nature Singapore.
25. Divyajyothi, M. G., Jopate, R., & Lenin, J. (2025). 19 The Future of Trust. Edge AI for Industry 5.0 and Healthcare 5.0 Applications, 269.