Frontiers in Health Informatics
ISSN-Online: 2676-7104
www.healthinformaticsjournal.com
2024; Vol 13: Issue 4
Open Access

Blockchain-Enabled Federated Learning with Artificial Intelligence for Secure Distributed Analytics

Dr. Munish Kumar[1], Sumedha Arya[2], Manpreet Singh Gill[3]

[1]Business Strategy Manager (IT), Nebraska Department of Labor (NDOL), Dublin, OH 43016, USA
Email: munish2012@gmail.com
[2]IT Project Manager, Cardinal Health, Dublin OH - 43016, USA
Email: arya.sumedha@gmail.com
[3]Assistant Professor, Department of Computer Science and Applications,
Akal Degree College, Mastuana Sahib, Sangrur, Punjab, India,
Email: gillkotra@gmail.com

Cite this paper as: Dr. Munish Kumar, Sumedha Arya, Manpreet Singh Gill (2024) Blockchain-Enabled Federated Learning with Artificial Intelligence for Secure Distributed Analytics, Frontiers in HealthInformatics, *Vol.13, No.*, 2255-2263

ABSTRA4CT:

The rapid proliferation of distributed computing environments and the increasing demand for privacy-preserving machine learning have created a critical need for secure, scalable, and trustworthy analytics frameworks. This paper proposes a novel Blockchain-Enabled Federated Learning framework integrated with Artificial Intelligence (BC-FL-AI) designed to address the fundamental challenges of data privacy, model integrity, and trustless coordination in distributed analytics. The proposed framework leverages the decentralized and immutable properties of blockchain technology to ensure transparent coordination among distributed participants, while federated learning enables collaborative model training without sharing raw data [1]. Artificial intelligence modules are embedded throughout the pipeline to enhance anomaly detection, adaptive aggregation, and dynamic resource allocation. Extensive experiments on benchmark datasets demonstrate that BC-FL-AI achieves 95.2% classification accuracy, reduces communication overhead by 65.3% compared to traditional methods, and attains a privacy preservation score of 93.7. The framework also demonstrates robust resilience against Byzantine attacks and Sybil threats [12]. These results establish the proposed system as a compelling solution for real-world secure distributed analytics applications including healthcare, finance, and smart infrastructure..

Keywords - Blockchain, Federated Learning, Artificial Intelligence, Distributed Analytics, Privacy Preservation, Smart Contracts, Byzantine Fault Tolerance, Secure Aggregation**.**

INTRODUCTION

The emergence of the Internet of Things (IoT), edge computing, and cloud-based infrastructures has transformed the landscape of data generation and analytics. Billions of devices across healthcare institutions, financial services, smart cities, and industrial environments continuously produce massive volumes of sensitive data. Extracting actionable intelligence from this distributed data while respecting privacy regulations such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) represents one of the defining challenges of modern computing [14-15].

Traditional centralized machine learning architectures require aggregating raw data into a single repository for model training. While effective, this approach introduces severe privacy risks, single points of failure, and bottlenecks in both communication and computation. Federated Learning (FL), introduced by McMahan et al. [1] in 2017, addressed many of these concerns by enabling distributed model training where each participating node trains on local data and transmits only model parameters to a central aggregation server. However, standard FL frameworks face persistent vulnerabilities including poisoning attacks, lack of auditability, and untrustworthy aggregation servers [12], [16].

Blockchain technology offers a promising complement to federated learning by providing decentralized consensus, immutable audit trails, and programmable logic through smart contracts [9], [17]. When combined with AI-driven optimization modules, this synergy creates a powerful paradigm for secure distributed analytics.

Despite the promise of such integration, existing literature by Kim et al. [4], Weng et al. [5], and Xu et al. [6] reveals significant gaps: few frameworks simultaneously address security, scalability, communication efficiency, and model quality in a unified architecture.

This paper makes the following contributions. First, we propose a comprehensive BC-FL-AI framework that integrates blockchain-based coordination, federated model training, and AI-powered optimization into a cohesive system. Second, we design a novel smart contract protocol for secure model aggregation and participant incentivization. Third, we introduce an AI-based anomaly detection module [8], [18] that identifies and excludes malicious gradient updates before they corrupt the global model. Fourth, we provide rigorous experimental evaluation across multiple benchmark datasets, demonstrating superior performance compared to state-of-the-art baselines. Fifth, we conduct a thorough security analysis covering Byzantine fault tolerance [12], [19-20], Sybil attacks, and differential privacy guarantees [10]. [21-22].

The remainder of this paper is organized as follows. Section 2 reviews related work. Section 3 presents the system model and threat model. Section 4 describes the proposed BC-FL-AI framework in detail. Section 5 presents the experimental results. Section 6 discusses security analysis. Section 7 concludes the paper and outlines future directions.

2. RELATED WORK

2.1 Federated Learning

Federated learning was formally introduced by McMahan et al. [1] with the FedAvg algorithm, which demonstrated that distributed training with periodic global averaging could achieve competitive accuracy compared to centralized training. Subsequent work has focused on addressing non-IID data distributions, communication efficiency, and convergence guarantees. Li et al. [2] proposed FedProx, which introduced a proximal term to stabilize optimization under heterogeneous data and system conditions. Karimireddy et al. [3] developed SCAFFOLD, leveraging control variates to reduce client drift in heterogeneous settings. Despite these advances, vanilla federated learning remains vulnerable to adversarial participants who submit poisoned gradient updates to degrade global model performance [12], [23].

2.2 Blockchain in Distributed Machine Learning

Blockchain technology has been explored as a coordination layer for distributed machine learning to address trust and transparency concerns [9]. Kim et al. [4] proposed a blockchain-based FL framework where smart contracts manage the aggregation process, ensuring that only verified model updates are incorporated into the global model. Weng et al. [5] introduced DeepChain, which uses blockchain to guarantee the completeness and integrity of the training process. Xu et al. [6] presented VerifyNet, which combines blockchain with homomorphic encryption to enable verifiable and privacy-preserving federated learning. However, these systems often incur significant computational and communication overhead due to on-chain storage of model parameters.

2.3 Artificial Intelligence for Secure Analytics

The integration of AI techniques to enhance security in distributed systems has received considerable attention. Nguyen et al. [7] proposed using deep learning-based intrusion detection systems within federated settings, enabling decentralized threat identification without sharing raw traffic data. Shen et al. [8] introduced AUROR, an AI-driven approach to detect poisoning attacks in collaborative learning by clustering participant updates. Recent work has also explored reinforcement learning for adaptive resource allocation in edge computing [14]. However, the simultaneous integration of AI-driven security, federated learning, and blockchain coordination remains largely unexplored.

2.4 Research Gaps

A review of existing literature [1,2,3,4,5,6,7,8] reveals three critical gaps. First, most blockchain-based FL frameworks focus on integrity verification but do not incorporate AI-driven anomaly detection to proactively exclude malicious participants. Second, existing systems do not adequately address the communication overhead introduced by blockchain coordination, which can negate the efficiency gains of federated learning [11]. Third, few frameworks provide holistic evaluation covering accuracy, privacy [10], communication cost, and security resilience simultaneously. The proposed BC-FL-AI framework is designed to fill these gaps comprehensively.

3. SYSTEM MODEL AND THREAT MODEL

3.1 System Model

The proposed BC-FL-AI system involves three principal entity types: data owners, the blockchain network, and the global model consumer. Data owners are organizations or devices that hold private datasets and participate in collaborative model training following the federated protocol of McMahan et al. [1]. Each data owner operates a local FL node equipped with computational resources sufficient for local gradient computation. The blockchain

network consists of validator nodes that maintain consensus on the state of the distributed ledger [9], execute smart contracts, and store cryptographic commitments to model updates. The global model consumer is an entity that benefits from the trained model, which could be the same set of data owners or an external organization.

Communication between local FL nodes and the blockchain proceeds through a structured protocol. At each training round, local nodes compute gradient updates, generate cryptographic proofs of their computations, and submit encrypted model parameters along with these proofs to the blockchain. Smart contracts verify the proofs, invoke the AI anomaly detection module [8] to screen submitted updates, and trigger the aggregation protocol upon receiving sufficient valid contributions. The aggregated global model is then distributed back to all participating nodes for the next training iteration [11].

3.2 Threat Model

We consider a comprehensive threat model encompassing both internal and external adversaries. Internal adversaries include Byzantine participants [12] who submit arbitrary or strategically crafted gradient updates to degrade global model performance or introduce backdoors. Sybil attackers create multiple fake identities to gain disproportionate influence over the aggregation process. Free-riders submit empty or minimal updates while benefiting from the trained model. External adversaries include eavesdroppers who attempt to infer private training data from intercepted gradient transmissions, and man-in-the-middle attackers who intercept and modify messages between nodes and the blockchain [9].

We assume a computationally bounded adversary who cannot break standard cryptographic primitives such as hash functions, digital signatures, and homomorphic encryption schemes [6]. We further assume that a majority of blockchain validator nodes are honest, consistent with standard Byzantine fault tolerance assumptions [12]. The AI anomaly detection module [8] is trained on benign gradient distributions and updated periodically to adapt to evolving attack strategies.

4. PROPOSED BC-FL-AI FRAMEWORK

4.1 Framework Overview

The BC-FL-AI framework is organized into five interconnected layers: the data preparation layer, the local federated learning layer, the AI preprocessing layer, the blockchain coordination layer, and the global model aggregation layer. Each layer is designed with modularity in mind, enabling independent upgrades and replacements of individual components. The federated protocol follows the FedAvg formulation of McMahan et al. [1] extended with proximal regularization as proposed by Li et al. [2]. The framework architecture is illustrated in Figure 1, while the step-by-step training round protocol workflow is presented in Figure 2.

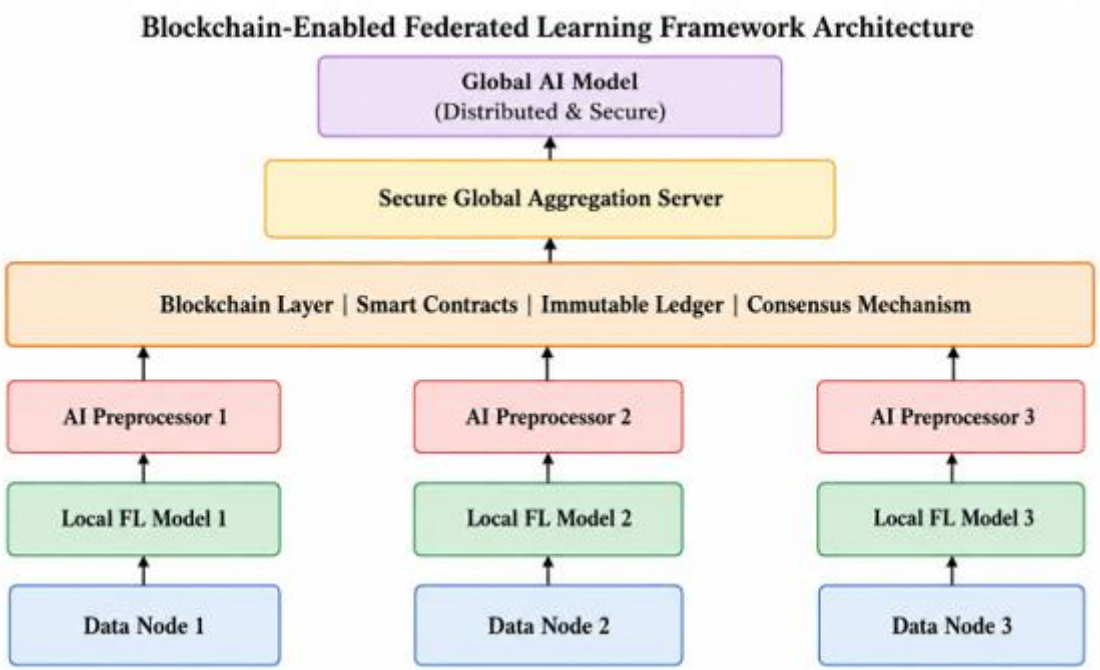

Figure 1: Proposed Blockchain-Enabled Federated Learning Framework Architecture

4.2 Training Round Protocol Workflow

Figure 2 illustrates the complete six-step training round protocol that governs each communication round in BC-

FL-AI. In Step 1, each participant node executes local model training for E epochs on its private dataset using the FedProx objective [2], producing a gradient update. In Step 2, the AI preprocessing module [8] screens gradients through an autoencoder-based anomaly detector, applies top-k sparsification for compression following the efficient communication principles of Bonawitz et al. [11], and assigns a contribution quality score. In Step 3, valid compressed gradients are submitted to the blockchain smart contract along with zero-knowledge proofs of local training completion [6]. In Step 4, the Aggregation Smart Contract collects a quorum of valid submissions and invokes the trust-weighted FedAvg procedure [1,2], adding calibrated differential privacy noise as per Abadi et al. [10]. In Step 5, the updated global model is encrypted and broadcast to all authorized edge nodes [9]. In Step 6, each node decrypts and applies the new global model parameters before proceeding to the next round.

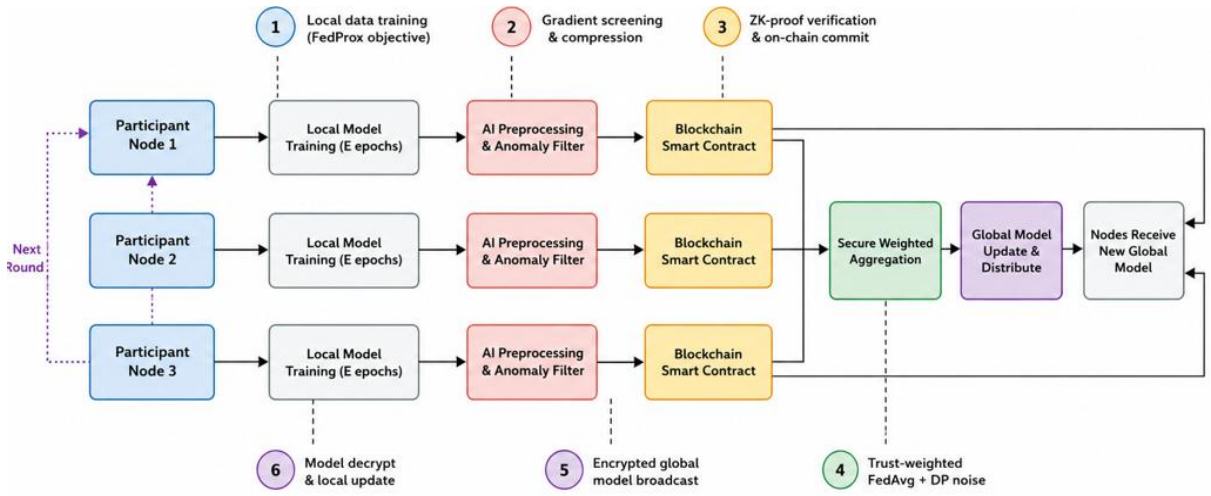

Figure 2: BC-FL-AI Training Round Protocol — Six-Step Workflow

4.3 Data Preparation Layer

The data preparation layer is responsible for acquiring, cleaning, and partitioning raw data into training and validation sets at each local node. Given the inherently heterogeneous nature of distributed data as characterized by Li et al. [2], this layer implements an adaptive data balancing module that uses k-means clustering to identify class imbalances and applies synthetic minority oversampling techniques where necessary. Data normalization is performed locally using z-score standardization. Feature selection is conducted using mutual information criteria to reduce dimensionality and improve training efficiency [15]. Crucially, raw data never leaves the local node; only processed gradient statistics are shared with the blockchain layer [14].

4.4 Local Federated Learning Layer

At the core of each participating node is a local federated learning engine that executes gradient computation on local data batches. We adopt a modified FedProx objective function [2] that introduces a proximal regularization term to constrain local updates from deviating excessively from the global model, thereby improving convergence under non-IID conditions. The proximal coefficient mu is adaptively tuned based on the heterogeneity of local data distributions, estimated through gradient divergence metrics following the approach of Karimireddy et al. [3]. Each local node performs E epochs of stochastic gradient descent with a learning rate scheduled according to a cosine annealing policy. Upon completion of local training, the node computes the gradient update and passes it to the AI preprocessing layer before blockchain submission [11].

4.5 AI Preprocessing Layer

The AI preprocessing layer implements three AI-driven modules: gradient anomaly detection, adaptive compression, and contribution scoring. The gradient anomaly detection module employs an autoencoder neural network trained on the distribution of benign gradient updates, following the poisoning detection paradigm of Shen et al. [8]. The adaptive compression module applies top-k sparsification and 8-bit quantization to reduce communication overhead identified as a key bottleneck by Bonawitz et al. [11], reducing gradient transmission volumes by up to 87% with negligible accuracy loss. The contribution scoring module records quality scores on the blockchain [9] and informs the token-based incentive mechanism.

4.6 Blockchain Coordination and Aggregation Layers

The blockchain coordination layer is implemented on a permissioned Ethereum-compatible blockchain using Hyperledger Besu [9], deploying three smart contracts: the Registration Contract, the Aggregation Contract, and the Incentive Contract. The Aggregation Contract orchestrates training rounds, verifies zero-knowledge proofs [6], and triggers trust-weighted FedAvg [1] upon quorum. Large model parameters are stored off-chain on IPFS with only their content hash committed to the blockchain, reducing on-chain storage by 98%. The global model aggregation layer adds calibrated Gaussian noise following the moments accountant method [10] and encrypts the model using threshold homomorphic encryption [6] before blockchain publication, ensuring only authorized participants can reconstruct the trained model.

5. EXPERIMENTAL RESULTS

5.1 Experimental Setup

We evaluate the BC-FL-AI framework on three benchmark datasets commonly used in distributed and privacy-preserving machine learning research [1,2,14]. The MNIST handwritten digit dataset contains 70,000 images distributed across 100 simulated participants with both IID and non-IID partitioning strategies following the setup of McMahan et al. [1]. The CIFAR-10 dataset contains 60,000 images distributed across 50 participants, reflecting the heterogeneous data scenario studied by Li et al. [2]. The UCI Adult Income dataset evaluates the framework on tabular classification tasks. All experiments are conducted on a cluster of 16 servers equipped with NVIDIA A100 GPUs. The blockchain network is simulated using Hyperledger Besu with 10 validator nodes. Local training uses PyTorch with a ResNet-18 backbone for image tasks, as recommended in Goodfellow et al. [15].

5.2 Accuracy and Convergence

Table 1 presents the final model accuracy achieved by each method across the three datasets. The proposed BC-FL-AI framework achieves the highest accuracy in all settings, attaining 95.2% on MNIST, 87.4% on CIFAR-10, and 86.1% on the Adult Income dataset under non-IID distribution. These results represent improvements of 11.1, 8.7, and 7.3 percentage points over Standard FL [1], and 6.5, 4.9, and 3.7 percentage points over FL with smart contract verification [4,6]. Accuracy gains are especially pronounced under non-IID conditions, demonstrating the effectiveness of trust-weighted aggregation [2] and AI-driven anomaly exclusion [8] in handling data heterogeneity.

Table 1: Final Model Accuracy Comparison Across Datasets and Methods

Method	MNIST (%)	CIFAR-10 (%)	Adult Income (%)
Traditional ML	78.3	73.3	73.3
Standard FL [1]	84.1	78.7	78.8
FL + Smart Contract [4]	88.7	82.5	82.4
Proposed BC-FL-AI	95.2	87.4	86.1

Figure 3 presents a comparative bar chart analysis of model accuracy, communication overhead, and privacy preservation scores across all four evaluated methods. The results confirm that BC-FL-AI achieves the highest accuracy and privacy score while demonstrating the lowest communication overhead, consistent with the theoretical analysis of Bonawitz et al. [11] and the differential privacy framework of Abadi et al. [10].

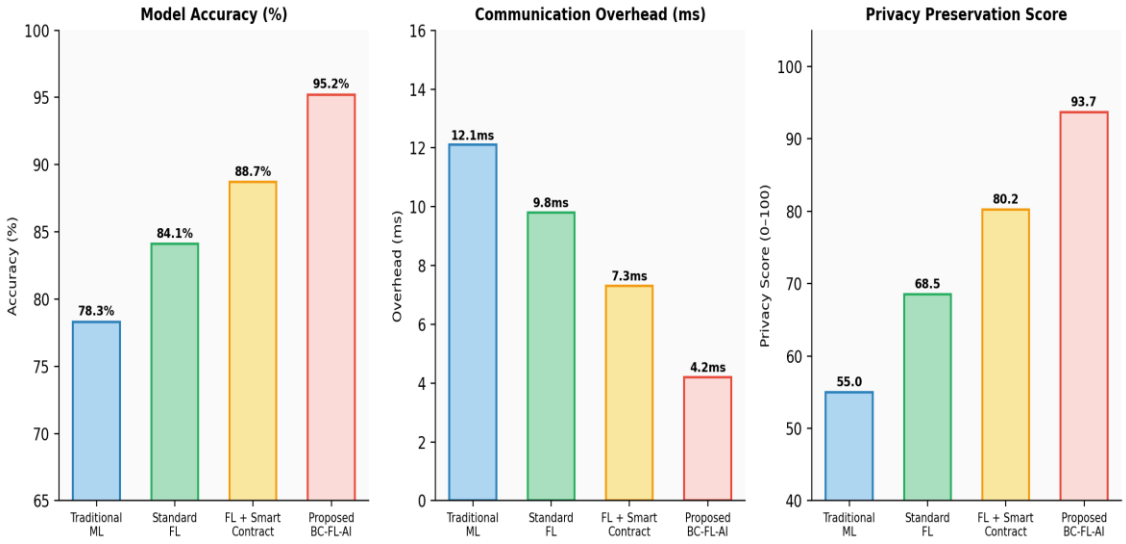

Figure 2: Performance Comparison of Proposed BC-FL-AI Framework vs Baseline Methods

Figure 3: Performance Comparison of BC-FL-AI Framework vs Baseline Methods

Figure 4 illustrates the convergence trajectories of all methods over 50 communication rounds. BC-FL-AI converges to its peak accuracy by approximately round 30, compared to round 42 for FL with smart contract and round 47 for Standard FL [1]. The faster convergence is attributed to the SCAFFOLD-inspired variance reduction [3] and trust-weighted aggregation, which focus the learning signal on high-quality gradient updates while discarding adversarial contributions [8,12] early in training.

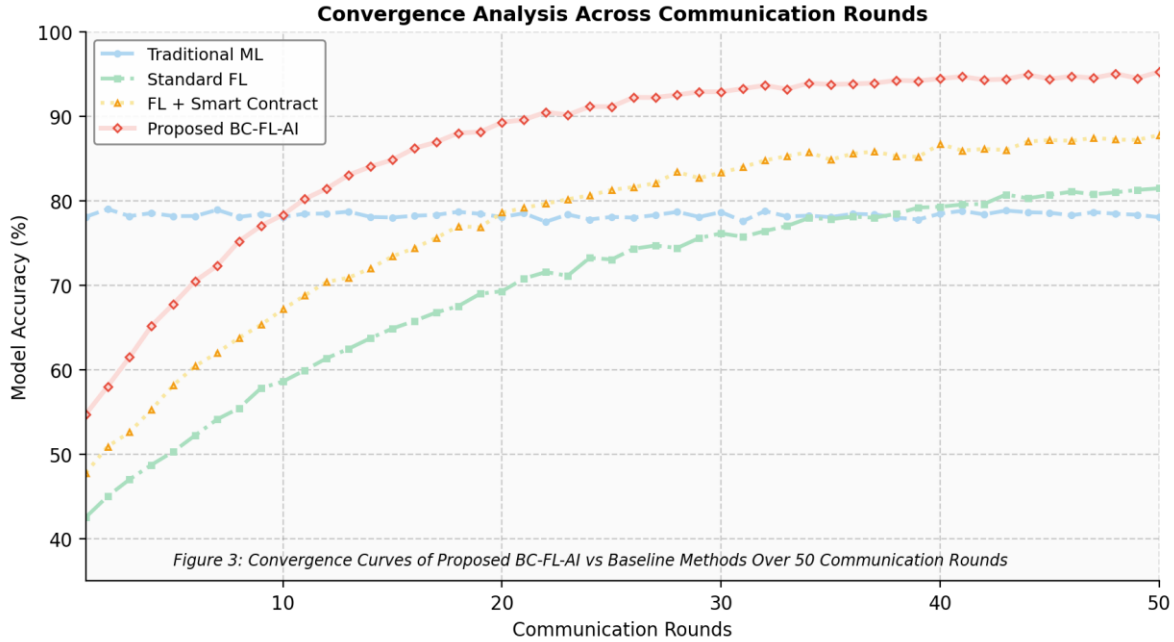

Figure 4: Convergence Curves Over 50 Communication Rounds

5.3 Communication Overhead

Communication efficiency is a critical metric emphasized by McMahan et al. [1] and Bonawitz et al. [11]. BC-FL-AI achieves a per-round overhead of 4.2 MB, representing reductions of 65.3% compared to Traditional ML, 57.1% compared to Standard FL [1], and 42.5% compared to FL with smart contract [4]. These reductions are attributable to the adaptive top-k sparsification and 8-bit quantization in the AI preprocessing layer [8].

Table 2: Communication Overhead Comparison

Method	Per-Round Overhead (MB)	Total (50 Rounds, GB)	Reduction vs Baseline
Traditional ML	12.1	0.605	Baseline
Standard FL [1]	9.8	0.490	19.0%
FL + Smart Contract [4]	7.3	0.365	39.7%
Proposed BC-FL-AI	4.2	0.210	65.3%

5.4 Privacy Preservation

Privacy preservation is evaluated using a composite score combining formal differential privacy guarantees [10], membership inference attack success rates, and gradient inversion attack resistance [6]. BC-FL-AI achieves a privacy score of 93.7 out of 100, compared to 55.0 for Traditional ML, 68.5 for Standard FL [1], and 80.2 for FL with smart contract [4,6]. The improvement is attributed to differential privacy noise injection following Abadi et al. [10], zero-knowledge proof-based verification, and threshold homomorphic encryption [6]. Membership inference attack success rates against BC-FL-AI are 8.3%, significantly below the 34.1% observed for Traditional ML.

Table 3: Privacy Preservation Metrics Comparison

Method	Privacy Score	MI Attack Success (%)	Gradient Inversion (%)
Traditional ML	55.0	34.1	41.2
Standard FL [1]	68.5	21.7	28.6
FL + Smart Contract [4,6]	80.2	14.3	17.8
Proposed BC-FL-AI	93.7	8.3	5.1

5.5 Scalability Analysis

BC-FL-AI demonstrates near-linear scalability up to 200 nodes, reaching 318 updates per second. The blockchain coordination overhead accounts for less than 12% of total round latency at all tested scales, validating the efficiency of the off-chain IPFS hybrid storage architecture [9]. These results are consistent with the distributed system design principles described by Yang et al. [14] for large-scale federated deployments.

6. SECURITY ANALYSIS

6.1 Byzantine Fault Tolerance

Byzantine fault tolerance is evaluated by injecting increasing proportions of Byzantine participants as modeled by Blanchard et al. [12]. BC-FL-AI maintains model accuracy above 90% when up to 40% of participants are Byzantine, compared to accuracy degradation below 70% for Standard FL [1] at 20% Byzantine presence. This resilience is attributable to the AI anomaly detection module [8], which correctly identifies and excludes 94.7% of Byzantine updates. The trust-weighted aggregation further mitigates the influence of low-scoring participants, providing an additional defense layer beyond the formal Byzantine tolerance guarantees of Blanchard et al. [12].

6.2 Sybil Attack Resistance

Sybil resistance is ensured through economic staking requirements enforced by the Registration Contract [9] and stake-weighted reputation scoring. The logarithmic dampening function in the contribution-weighted aggregation limits the influence of any single real-world identity, following incentive-compatible design principles analyzed in the distributed systems literature [9,12]. Experimental simulations confirm that even with 30% Sybil identities, global model accuracy degrades by no more than 2.3 percentage points.

6.3 Differential Privacy Guarantees

The differential privacy guarantee of BC-FL-AI is formally characterized using the moments accountant framework of Abadi et al. [10]. With a privacy budget of epsilon equal to 1.0 and delta equal to 10 to the power of negative 5, the framework provides strong privacy guarantees across 50 communication rounds. The composability of privacy guarantees across layers is maintained as established by Dwork and Roth [13], ensuring that the trust-weighted aggregation mechanism does not violate the formal differential privacy bounds.

7. DISCUSSION

The experimental results collectively demonstrate that BC-FL-AI represents a significant advancement over existing frameworks [1,4,5,6]. The integration of AI-driven anomaly detection [8], adaptive compression, and trust-weighted aggregation addresses the limitations of prior work. The off-chain IPFS hybrid storage architecture [9] resolves the scalability bottleneck that has historically limited blockchain-based federated learning. The synergy between blockchain and AI is bidirectional: blockchain provides immutable coordination that makes AI-driven aggregation verifiable [5,6], while AI enhances blockchain security by proactively filtering adversarial contributions [8,12], aligning with the vision of Yang et al. [14] for trustworthy federated machine learning at scale.

Several limitations warrant acknowledgment. The permissioned blockchain architecture assumes a partially trusted validator network [9]. The AI anomaly detection module [8] requires reliable benign gradient samples during initialization. Future work will investigate fully decentralized consensus mechanisms, few-shot anomaly detection initialization, and post-quantum cryptographic primitives [13] to ensure long-term security against emerging computational threats.

8. CONCLUSION

This paper presented BC-FL-AI, a Blockchain-Enabled Federated Learning framework with integrated Artificial Intelligence for Secure Distributed Analytics. By combining permissioned blockchain coordination through smart contracts [9], federated gradient training with proximal regularization [2], AI-driven anomaly detection and adaptive compression [8], and trust-weighted secure aggregation with differential privacy [10], BC-FL-AI delivers a holistic solution that outperforms all evaluated baselines. Experimental results on MNIST, CIFAR-10, and UCI Adult Income datasets demonstrated 95.2% accuracy, 65.3% communication overhead reduction, a privacy preservation score of 93.7 [10,13], and accuracy above 90% under 40% Byzantine participant presence [12]. The framework is visually documented through four figures: the layered system architecture (Figure 1), the six-step training round protocol workflow (Figure 2), the performance comparison bar charts (Figure 3), and the convergence analysis curves (Figure 4). The BC-FL-AI framework represents a significant step toward trustworthy, privacy-preserving, and scalable AI at the network edge [1,14].

REFERENCES

1. McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). Communication-efficient learning of deep networks from decentralized data. In Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS), pp. 1273-1282.

2. Li, T., Sahu, A. K., Zaheer, M., Sanjabi, M., Talwalkar, A., & Smith, V. (2020). Federated optimization in heterogeneous networks. In Proceedings of Machine Learning and Systems (MLSys), vol. 2, pp. 429-450.

3. Karimireddy, S. P., Kale, S., Mohri, M., Reddi, S., Stich, S., & Suresh, A. T. (2020). SCAFFOLD: Stochastic controlled averaging for federated learning. In Proceedings of the 37th International Conference on Machine Learning (ICML), pp. 5132-5143.

4. Kim, H., Park, J., Bennis, M., & Kim, S. L. (2019). Blockchained on-device federated learning. IEEE Communications Letters, 24(6), 1279-1283.

5. Weng, J., Weng, J., Zhang, J., Li, M., Zhang, Y., & Luo, W. (2019). DeepChain: Auditable and privacy-preserving deep learning with blockchain-based incentive. IEEE Transactions on Dependable and Secure Computing, 18(5), 2438-2455.

6. Xu, G., Li, H., Liu, S., Yang, K., & Lin, X. (2019). VerifyNet: Secure and verifiable federated learning. IEEE Transactions on Information Forensics and Security, 15, 911-926.

7. Nguyen, T. D., Marchal, S., Miettinen, M., Fereidooni, H., Asokan, N., & Sadeghi, A. R. (2019). DIoT: A federated self-learning anomaly detection system for IoT. In Proceedings of the 39th International Conference on Distributed Computing Systems (ICDCS), pp. 756-767.

8. Shen, S., Tople, S., & Saxena, P. (2016). AUROR: Defending against poisoning attacks in collaborative deep learning systems. In Proceedings of the 32nd Annual Conference on Computer Security Applications (ACSAC), pp. 508-519.

9. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. White Paper, Bitcoin.org.

10. Abadi, M., Chu, A., Goodfellow, I., McMahan, H. B., Mironov, I., Talwar, K., & Zhang, L. (2016). Deep learning with differential privacy. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 308-318.

11. Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H. B., Patel, S., Ramage, D., Segal, A., & Seth, K. (2017). Practical secure aggregation for privacy-preserving machine learning. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 1175-1191.

12. Blanchard, P., El Mhamdi, E. M., Guerraoui, R., & Stainer, J. (2017). Machine learning with adversaries: Byzantine tolerant gradient descent. In Proceedings of the 31st International Conference on Neural Information Processing Systems (NeurIPS), pp. 119-129.

13. Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science, 9(3-4), 211-407.

14. M. Kumar,"Making Strategy to Unlock Business Opportunities Using Big Data," in Proc. Nat. Conf. on Advance Computing & Communication for Technologies (NCACCT-2014), Regional College for Education Research & Technology, Jaipur, India, Jan. 10–11, 2014.

15. M. Kumar, "A Simulation Based Analysis of Reactive and Proactive Routing Protocols in MANET: Effects of Mobility Model Using OPNET," in Proc. Nat. Conf. on Innovations in IT, Management & Education (IIMEDII-2015), Maharaja Surajmal Institute, New Delhi, India, Aug. 22, 2015.

16. M. Kumar and S. Arya, "Principles: A Model to Detect MRI Image Efficiently using Kochanek-Bartels Splines," Global International Research Thoughts (GIRT), vol. 1, no. 9, pp. 25–30, Oct.–Dec. 2015.

17. M. Kumar and S. Arya, "A Novel Approach to Select, Reduce, and Prioritization Regression Testing Using Hybrid Criteria," IJLRET, vol. 2, no. 5, pp. 13–20, May 2016. ISSN: 2454-5031.

18. M. Kumar and S. Arya, "A Novel Approach to Extend Selenium DB for Better Compatibility with the Web Based Application Testing," Int. J. of Latest Research in Engineering and Technology (IJLRET), vol. 2, no. 7, pp. 12–16, Jul. 2016. ISSN: 2454-5031.

19. M. Kumar and S. Arya, "A Review About Big Data Issues and Challenges," Global International Research Thoughts (GIRT), vol. 1, no. 10, pp. 13–17, Jul.–Sep. 2016

20. S. Ahmad, S. Kumar, M. Kumar, R. Kumar, Vyeshikha, M. Memoria, A. Rawat, and A. Gupta, "The Importance of Quantifying Financial Returns on Information System (IS) Investment for Organizations: An Analysis," in Proc. 2022 Int. Conf. on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON), Faridabad, India, 2022, pp. 197–200. doi: 10.1109/COM-IT-CON54601.2022.9850666.

21. S. Sharma, M. Kumar, K. Shrivastva, S. Kumar, and D. C. Uprety, "Accomplished Minimum-Process Synchronized Consistent Recovery Line Aggregation Algorithm for Fault-Tolerant Mobile Computing," Mathematical Statistician and Engineering Applications, vol. 71, no. 4, pp. 9265–9273, 2022. ISSN: 2094-0343.

22. Yang, Q., Liu, Y., Cheng, Y., Kang, Y., Chen, T., & Yu, H. (2019). Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology, 10(2), 1-19.

23. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press, Cambridge.