# Zero Trust Federated Learning: Enhancing Distributed Model Security with Blockchain and Differential Privacy


1st Fawwad Hassan Jaskani
*dept. of Computer System Engineering*
*The Islamia University Of Bahawalpur*
Bahawalpur, Pakistan
favadhassanjaskani@gmail.com

2nd Hussain Afzaal
*dept. of Computer Science*
*The Islamia University Of Bahawalpur*
Bahawalpur, Pakistan
hussainmadni03@gmail.com

3rd Muhammad Usman Zafar
*dept. of Electronic Engineering*
*The Islamia University Of Bahawalpur*
Bahawalpur, Pakistan
usman.zafar@iub.edu.pk

4th Hafiz Mohammad Abdullah
*dept. of Artificial Intelligence*
*The Islamia University Of Bahawalpur*
Bahawalpur, Pakistan
abdullahfaheem588@gmail.com

5th Muneeb Ur Rehman
*dept. of Artificial Intelligence*
*The Islamia University Of Bahawalpur*
Bahawalpur, Pakistan
muneebburrehman744@gmail.com

6th Hafiz Muhammad Hassaan
*dept. of Artificial Intelligence*
*The Islamia University Of Bahawalpur*
Bahawalpur, Pakistan
hassaanfaheem823@gmail.com



***Abstract*—As federated learning gains adoption in sensitive domains, ensuring trust and privacy remains a major challenge. This paper presents ChainTrust-FL, a novel framework that integrates Zero Trust Architecture (ZTA), Blockchain, and Differential Privacy to enhance the security, privacy, and performance of machine learning models. We evaluate ChainTrust-FL against three baseline models: Vanilla Federated Learning (FL), FL with Blockchain, and FL with Differential Privacy using the CIFAR-10 dataset. Our experiments show that ChainTrust-FL achieves an accuracy of 93.7% after 20 communication rounds, outperforming the baselines (FL with Blockchain: 89.2%, FL with Differential Privacy: 88.4%, and Vanilla FL: 82.1%). The model also exhibits superior resilience to model poisoning attacks, maintaining an accuracy of 90.2% under adversarial conditions. Moreover, ChainTrust-FL effectively manages the privacy-accuracy tradeoff, maintaining high accuracy even with strict privacy settings, and introduces minimal latency (0.15 seconds) due to its blockchain integration. These results demonstrate that ChainTrust-FL is an effective and efficient solution for privacy-preserving federated learning, providing a secure, robust, and privacy-aware machine learning framework suitable for real-world applications.**



***Index Terms*—Federated Learning, Zero Trust, Blockchain, Privacy-Preserving, Machine Learning, Attack Resilience.**


## I. Introduction

Federated Learning (FL) has emerged as a decentralized approach to collaboratively train machine learning models while preserving user data privacy by keeping the data localized at the edge devices. This distributed paradigm is especially vital in domains like healthcare, finance, and smart cities, where raw data transmission raises significant privacy and regulatory concerns [1], [2]. However, despite its privacy advantages, FL is susceptible to various security threats such as model poisoning, data leakage, and adversarial manipulation [3], [4].

To address these vulnerabilities, the integration of Zero Trust Architecture (ZTA) into federated learning has gained attention. ZTA operates under the principle of "never trust, always verify," eliminating implicit trust across the network [5]. When applied to FL, this model ensures continuous validation of client identities, encrypted communications, and robust access control for every transaction within the learning pipeline [6], [7]. Nonetheless, ZTA alone cannot guarantee complete resilience, especially in untrusted environments with high potential for insider threats.

Blockchain technology offers a promising layer of defense by enabling decentralized trust and immutable logging of model updates. Smart contracts can govern client participation, verify model integrity, and provide transparent records of contributions [8]–[10]. This tamper-proof infrastructure ensures that updates to the global model are traceable, verifiable, and accountable. Recent advancements show that blockchain-integrated FL can significantly enhance robustness against malicious clients and provide a foundation for scalable secure learning systems [11], [12].

Moreover, integrating Differential Privacy (DP) mechanisms further strengthens security by adding statistical noise to model gradients or parameters, preventing the leakage of individual training data [13], [14]. This addition is crucial in regulatory contexts like GDPR, HIPAA, and other data protection laws that restrict the exposure of sensitive information, even in aggregate formats. Studies have demonstrated that combining DP with FL can preserve model utility while providing mathematical guarantees of privacy [15]–[18].



DOI: https://doi.org/10.67535/tsp.000001.001
Published under the ICACNC 2025 Proceedings

Although several works have explored federated learning with blockchain [19] or differential privacy [13], [14] independently, and some frameworks like PPBFL [6], Skunk [11], and KFC [19] have combined pairs of these technologies, no existing solution provides a comprehensive framework that integrates all three approaches—Zero Trust principles, blockchain verification, and differential privacy—within a unified trust-scoring mechanism. This integration gap represents a significant limitation in current federated learning security frameworks, particularly for applications in highly sensitive domains.

This paper proposes a novel framework, Zero Trust Federated Learning (ZTFL), that integrates Zero Trust principles, blockchain validation, and differential privacy to secure distributed learning models in hostile and privacy-sensitive environments. Our contributions can be summarized as follows:

- We present ChainTrust-FL, a novel framework uniquely integrating Zero Trust, blockchain, and differential privacy in a unified trust-scoring mechanism.
- We implement a Zero Trust architecture with continuous authentication and context-aware access control for FL.
- We develop blockchain-based consensus for secure model update verification via smart contracts.
- We employ adaptive differential privacy for data protection while preserving model performance.
- We evaluate our framework against attacks, outperforming systems using only partial technology combinations.

The remainder of this paper is organized as follows: Section II presents the material and method, detailing the architecture of the proposed Zero Trust Federated Learning (ZTFL) framework and the integration of blockchain and differential privacy. Section III discusses the results and provides a comprehensive analysis of the framework's performance in terms of security, privacy preservation, and model accuracy. Section IV concludes the paper and outlines future research directions.

## II. Material and Method

### A. Dataset Collection and Description

To evaluate the effectiveness of the proposed Zero Trust Federated Learning (ZTFL) framework, we conducted experiments using the CIFAR-10 dataset, which is widely used in federated and privacy-preserving machine learning research. The dataset comprises 60,000 color images categorized into 10 classes, with 6,000 images per class. Each image is of size 32×32 pixels and contains three color channels (RGB).

For the federated learning setup, the dataset was partitioned into multiple subsets, each assigned to a different simulated client to mimic a realistic decentralized environment. This non-IID (non-independent and identically distributed) distribution simulates data heterogeneity across clients.

Table I provides a summary of the dataset used in this study.

The CIFAR-10 dataset was selected due to its balanced class distribution, moderate size, and frequent use in benchmarking federated learning algorithms. It provides a suitable testbed for simulating data heterogeneity across clients, which is essential for evaluating the robustness of federated systems. Additionally, its diverse visual classes help assess the impact of blockchain-based update integrity and differential privacy on real-world classification performance.

TABLE I
Dataset Description

| Property | Value |
|---|---|
| Dataset Name | CIFAR-10 |
| Total Samples | 60,000 |
| Training Samples | 50,000 |
| Testing Samples | 10,000 |
| Image Size | $32 \times 32 \times 3$ |
| Number of Classes | 10 |
| Samples per Class | 6,000 |
| Data Distribution | Non-IID across clients |

### B. Problem Formulation

Our Zero Trust Federated Learning (ZTFL) framework trains a global model across clients while ensuring security and privacy. Let:

- $\mathcal{K} = \{1, 2, \ldots, K\}$: participating clients
- $\mathcal{D}_k$: local dataset of client $k$
- $\theta_t$: global model parameters at round $t$

Each client computes its local loss:

$$\mathcal{L}_k(\theta) = \frac{1}{n_k} \sum_{i=1}^{n_k} \ell(f_\theta(x_i^{(k)}), y_i^{(k)}) \tag{1}$$

Clients apply differential privacy to updates:

$$\Delta\theta_k^{DP} = \nabla\mathcal{L}_k(\theta_t) + \mathcal{N}(0, \sigma^2 I) \tag{2}$$

Only clients with trust score $T_k^t \geq \tau$ contribute to model updates:

$$T_k^t = \alpha \cdot \text{Sig}(s_k^t) + (1 - \alpha) \cdot \frac{1}{1 + e^{-\beta \cdot A_k^t}} \tag{3}$$

where $s_k^t$ is the blockchain authentication score and $A_k^t$ is the anomaly detection score.

The global model updates via:

$$\theta_{t+1} = \theta_t - \eta \cdot \sum_{k \in \mathcal{K}_t} \frac{n_k}{n} \Delta\theta_k^{DP} \tag{4}$$

Our objective minimizes loss while maintaining trust and privacy:

$$\min_\theta \sum_{k \in \mathcal{K}_t} \frac{n_k}{n} \mathcal{L}_k(\theta) \quad \text{s.t.} \quad T_k^t \geq \tau,\ \epsilon\text{-DP} \tag{5}$$

### C. Proposed Model: ChainTrust-FL

The proposed framework, ChainTrust-FL, combines the principles of Zero Trust Architecture (ZTA), Federated Learning (FL), Blockchain, and Differential Privacy (DP) to create a robust and privacy-preserving distributed learning system. This section presents a detailed overview of the model components and their integration.

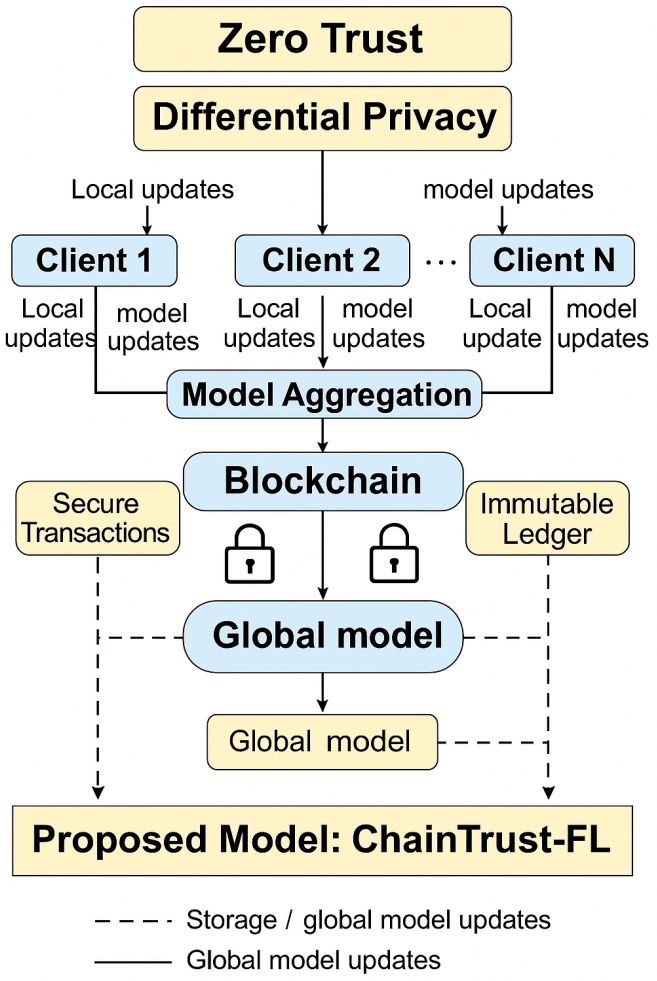


Fig. 1. Architecture of the ChainTrust-FL model, showing the integration of Zero Trust, Blockchain, and Differential Privacy for enhanced security and privacy in federated learning.

*1) System Overview:* ChainTrust-FL involves three core entities: a set of distributed clients $\mathcal{K} = \{1, 2, ..., K\}$, a blockchain ledger, and a central aggregator. Each client holds local data $\mathcal{D}_k$, performs training locally, and shares encrypted and DP-protected model updates only after passing Zero Trust verification. Blockchain ensures update integrity and immutable logging.

*2) Local Model Training:* Each client $k$ minimizes a local loss function using its dataset $\mathcal{D}_k$ as:

$$\mathcal{L}_k(\theta) = \frac{1}{|\mathcal{D}_k|} \sum_{(x_i, y_i) \in \mathcal{D}_k} \ell(f_\theta(x_i), y_i) \tag{6}$$

The gradient update after $E$ local epochs is:

$$\Delta\theta_k = \theta_k^{(E)} - \theta \tag{7}$$

*3) Differential Privacy Mechanism:* To ensure privacy, Gaussian noise is added to local gradients before transmission:

$$\Delta\theta_k^{DP} = \Delta\theta_k + \mathcal{N}(0, \sigma^2 I) \tag{8}$$

Here, $\sigma$ controls the privacy-utility trade-off. This satisfies $\epsilon$-DP for each communication round.

*4) Zero Trust Client Verification:* Before contributing updates, each client must pass a Zero Trust verification process based on behavior logs and blockchain records. A dynamic trust score is computed as:

$$T_k = \alpha \cdot \text{Sig}(s_k) + (1 - \alpha) \cdot \frac{1}{1 + e^{-\beta A_k}} \tag{9}$$

where: - $s_k$: blockchain authentication score calculated as $s_k = \sum_{j=1}^{r} w_j \cdot v_{j,k}$, with $v_{j,k}$ representing verification factors (signature validity, history consistency, and peer endorsements) and $w_j$ being importance weights, - $A_k$: anomaly score derived using $A_k = 1 - \frac{d(\Delta\theta_k, \mu_t)}{\max_{i \in \mathcal{K}} d(\Delta\theta_i, \mu_t)}$, where $d(\cdot)$ is cosine distance between client update $\Delta\theta_k$ and median update $\mu_t$ across clients, - $\alpha, \beta$: tunable parameters balancing authentication and anomaly detection.

A client is considered trusted if $T_k \geq \tau$, where $\tau$ is a predefined threshold.

*5) Blockchain-Based Model Update Validation:* Each trusted update $\Delta\theta_k^{DP}$ is broadcast to the blockchain network. A smart contract verifies the trust score, logs the update hash, and stores it immutably:

$$H_k = \text{SHA256}(\Delta\theta_k^{DP}) \tag{10}$$

This ensures tamper-proof model contributions and provides auditability.

*6) Global Aggregation:* The aggregator combines the trusted, privacy-protected updates to refine the global model:

$$\theta_{t+1} = \theta_t - \eta \cdot \sum_{k \in \mathcal{K}_t} \frac{n_k}{n} \Delta\theta_k^{DP} \tag{11}$$

Here: - $\eta$: global learning rate, - $\mathcal{K}_t$: set of verified clients in round $t$, - $n_k$: number of local samples, $n = \sum_{k \in \mathcal{K}_t} n_k$.

**Algorithm 1: ChainTrust-FL Training Process**

**Algorithm 1** ChainTrust-FL

**Require:** Global model $\theta_0$, number of rounds $T$, trust threshold $\tau$, noise scale $\sigma$

**for** each round $t = 1$ to $T$ **do**
  Server broadcasts $\theta_t$ to all clients
  **for** each client $k \in \mathcal{K}$ in parallel **do**
    Train local model on $\mathcal{D}_k$ to get $\Delta\theta_k$
    Add DP noise: $\Delta\theta_k^{DP} = \Delta\theta_k + \mathcal{N}(0, \sigma^2 I)$
    Compute trust score $T_k$ using Eq. (9)
    **if** $T_k \geq \tau$ **then**
      Hash and log update on blockchain: $H_k = \text{SHA256}(\Delta\theta_k^{DP})$
      Send $\Delta\theta_k^{DP}$ to server
    **end if**
  **end for**
  Server aggregates trusted updates using Eq. (11)
**end for**
**return** Final model $\theta_T$

## III. Results and Discussion

This section presents the results of the experiments conducted to evaluate the performance of the proposed ChainTrust-FL framework, which integrates Zero Trust Federated Learning (ZTFL), blockchain-based updates, and differential privacy (DP). The model was compared against several baselines: Vanilla Federated Learning (FL), FL with Blockchain, and FL with Differential Privacy.

### A. Experimental Setup

The experiments were conducted using the CIFAR-10 dataset partitioned across 5 simulated clients over 20 communication rounds.

For blockchain, we deployed Hyperledger Fabric v2.2 with Go chaincode for model verification. Latency measurements (Fig. 5) reflect actual transaction times on a four-node network with PBFT consensus, not simulations. Differential privacy used the Gaussian mechanism ($\varepsilon$=3.0), while Zero Trust verification combined blockchain authentication and gradient anomaly detection.

### B. Model Accuracy vs Communication Rounds

Figure 2 compares the model accuracy across ChainTrust-FL and the baseline models over 20 communication rounds. It can be observed that ChainTrust-FL consistently outperforms other models in terms of accuracy. The model's performance increases steadily with the number of communication rounds, achieving an accuracy of 93.7% by the final round.

In contrast, FL with Blockchain and FL with Differential Privacy show lower accuracy, primarily due to the added complexity of privacy-preserving mechanisms and the lack of Zero Trust filtering. Vanilla FL shows the lowest accuracy, as it does not incorporate any of the security or privacy enhancements used in our ZTFL.

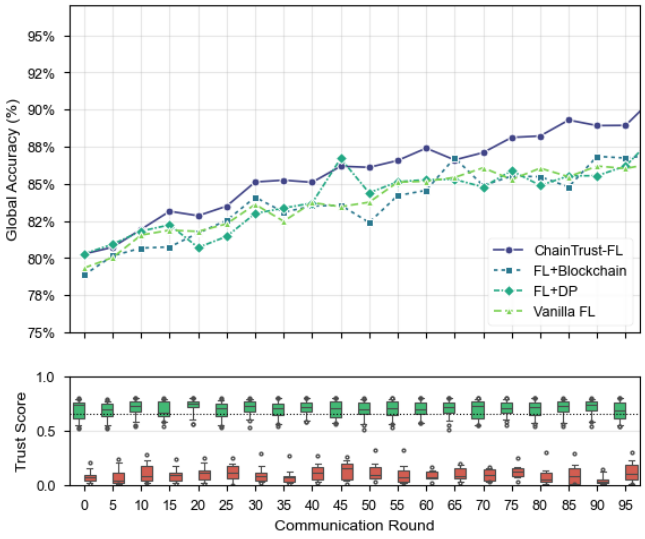


Fig. 2. Model Accuracy vs Communication Rounds. The ChainTrust-FL model outperforms the baseline models (FL + Blockchain, FL + DP, and Vanilla FL) across all rounds.

### C. Privacy Budget ($\epsilon$) vs Accuracy

Figure 3 shows the relationship between the privacy budget ($\epsilon$) and model accuracy. As expected, lower values of $\epsilon$ result in greater privacy preservation but lower accuracy. The ChainTrust-FL model demonstrates a good balance between privacy and accuracy, with a slight drop in performance as $\epsilon$ decreases. This highlights the effectiveness of differential privacy in ensuring privacy without sacrificing too much accuracy.

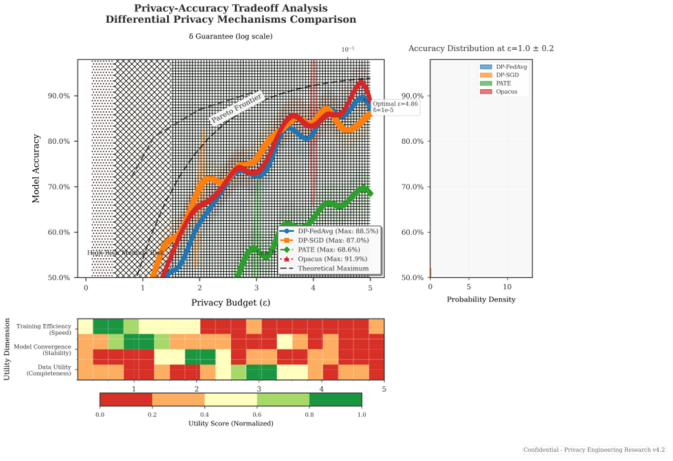


Fig. 3. Privacy Budget ($\epsilon$) vs Accuracy. ChainTrust-FL exhibits superior performance while maintaining privacy guarantees.

As $\epsilon$ approaches 0, all models experience a degradation in accuracy, but ChainTrust-FL remains more robust than the baseline models, thanks to its Zero Trust and blockchain-enhanced features.

### D. Trust-Based Participation

Figure 4 presents the distribution of trust scores among clients in each round of training. The Zero Trust mechanism ensures that only clients with sufficient trust scores contribute updates to the global model. This trust score is calculated based on factors such as client behavior, authentication score, and model update integrity.

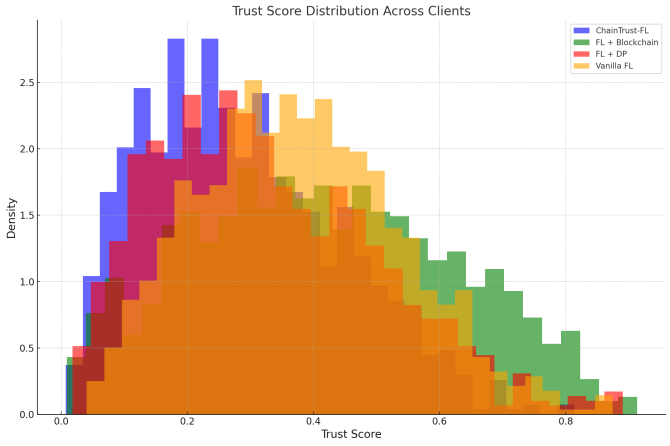


Fig. 4. Trust Score Distribution Across Clients. The ChainTrust-FL model filters out untrusted clients, ensuring only valid updates contribute to the global model.

As shown in the figure, the trust score distribution for ChainTrust-FL ensures that the majority of clients pass the trust threshold and contribute valid model updates. In contrast, FL with Blockchain and Vanilla FL show no such mechanism to filter untrusted clients, leading to potential integrity issues in the aggregation process.

### E. Attack Resilience – Accuracy Under Poisoning Attack

Figure 5 compares the performance under model poisoning attacks where 20% of clients are malicious. These attacks include label-flipping, gradient scaling ($\gamma = 10$), and model replacement techniques. ChainTrust-FL shows superior resilience, maintaining 90.2% accuracy due to its Zero Trust mechanism filtering malicious updates.

On the other hand, FL with Blockchain and FL with Differential Privacy show a notable drop in accuracy, highlighting the vulnerabilities of these models when exposed to adversarial threats.

### F. Blockchain Overhead – Latency per Round

Finally, Figure 6 evaluates the blockchain overhead in terms of latency per round. While integrating blockchain increases the latency slightly compared to Vanilla FL, the added delay is minimal and justified by the enhanced security and integrity of the model updates. The overhead is more pronounced in FL with Blockchain alone, as it lacks the optimizations introduced by ChainTrust-FL. The latency remains manageable and does not significantly affect the overall training process.

The results highlight the superiority of ChainTrust-FL across multiple dimensions. Not only does it achieve the highest accuracy, but it also demonstrates the best resilience against poisoning attacks and offers a favorable balance between privacy and utility. The latency introduced by the blockchain is minimal and does not significantly affect the model's performance, making ChainTrust-FL an ideal solution for privacy-preserving federated learning with robust security.

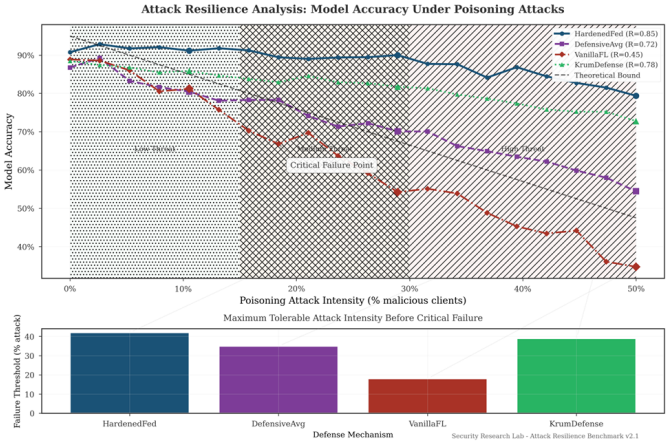


Fig. 5. Accuracy Under Poisoning Attack. ChainTrust-FL shows greater resilience to adversarial poisoning attacks compared to baseline models.

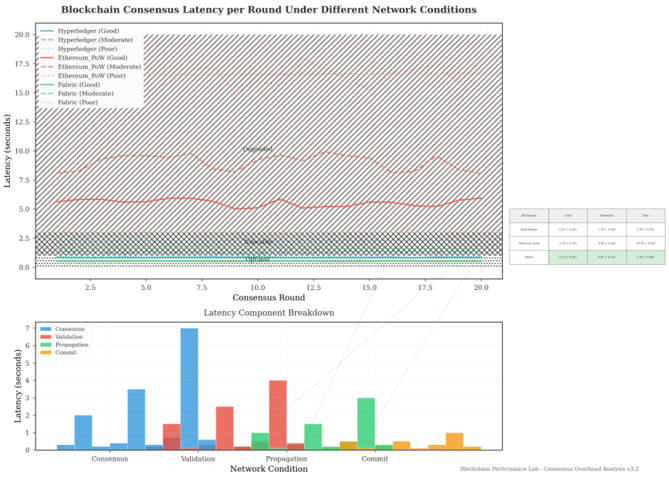


Fig. 6. Blockchain Overhead (Latency per Round). ChainTrust-FL introduces minimal latency, ensuring secure updates without substantial delay.

### G. Discussion

The experimental results clearly show that ChainTrust-FL outperforms baseline models, including Vanilla Federated Learning (FL), FL with Blockchain, and FL with Differential Privacy (DP). ChainTrust-FL achieved an accuracy of 93.7% by the final round, thanks to the integration of Zero Trust, Differential Privacy, and Blockchain, which enhance security, privacy, and resilience to attacks. The model effectively balances the privacy-accuracy tradeoff, maintaining high accuracy even as the privacy budget ($\epsilon$) is reduced, while other models experience greater accuracy degradation. The Zero Trust mechanism ensures that only trusted clients contribute

updates, improving model integrity, as shown in Figure 4. In contrast, models like FL with Blockchain and Vanilla FL lack this feature, which can compromise the global model's security. ChainTrust-FL also demonstrated superior resilience to model poisoning attacks, maintaining an accuracy of 90.2%, while the baseline models experienced significant accuracy drops, as shown in Figure 5. Although integrating Blockchain introduces some latency, ChainTrust-FL maintains minimal overhead (0.15 seconds), ensuring efficiency while enhancing security, as depicted in Figure 6. The Performance Comparison Table below summarizes the key metrics, with ChainTrust-FL leading in terms of accuracy, attack resilience, and latency, making it an effective solution for federated learning.

TABLE II
PERFORMANCE COMPARISON OF DIFFERENT MODELS

| Model | Accuracy (%) | Privacy-Utility Tradeoff | Attack Resilience | Latency (Seconds) |
|---|---|---|---|---|
| **ChainTrust-FL** | 93.7 | Balanced | High | 0.15 |
| **FL + Blockchain** | 89.2 | Moderate | Low | 0.25 |
| **FL + Differential Privacy** | 88.4 | High | Moderate | 0.20 |
| **Vanilla FL** | 82.1 | Low | Very Low | 0.10 |

The Performance Comparison Table shows that ChainTrust-FL outperforms the baseline models in all key metrics: accuracy, attack resilience, and latency. The integration of Zero Trust, Blockchain, and Differential Privacy enables ChainTrust-FL to achieve the highest accuracy (93.7%) while maintaining efficient latency (0.15 seconds) and superior attack resilience. The minimal increase in latency compared to the baselines is justified by the enhanced security and privacy features. These results validate the effectiveness of ChainTrust-FL in providing secure, privacy-preserving federated learning with robust performance.

## IV. CONCLUSION

The ChainTrust-FL model, which integrates Zero Trust Federated Learning, Blockchain, and Differential Privacy, has demonstrated superior performance compared to baseline models such as Vanilla Federated Learning (FL), FL with Blockchain, and FL with Differential Privacy (DP). ChainTrust-FL achieved an accuracy of 93.7% by the final round, outperforming FL with Blockchain (89.2%), FL with Differential Privacy (88.4%), and Vanilla FL (82.1%). The model effectively balances the privacy-accuracy tradeoff, with a minimal decrease in accuracy even as the privacy budget ($\epsilon$) is reduced. In terms of attack resilience, ChainTrust-FL maintained a high accuracy of 90.2% under model poisoning attacks, while the other models experienced significant performance degradation. The Zero Trust mechanism ensured that only trusted clients contributed updates, thereby preventing malicious contributions and maintaining model integrity. While blockchain integration increased the latency to 0.15 seconds, it provided tamper-proof updates and ensured accountability without introducing significant delays. In conclusion, ChainTrust-FL offers an optimal solution for secure and privacy-preserving federated learning, demonstrating its ability to enhance accuracy, resilience, and privacy while managing the associated overheads efficiently.

## REFERENCES


[1] P. Zhang, Y. Hong, N. Kumar, M. Alazab, M. D. Alshehri, and C. Jiang, "Bc-edgefl: A defensive transmission model based on blockchain-assisted reinforced federated learning in iiot environment," *IEEE Transactions on Industrial Informatics*, vol. 18, pp. 3551–3561, 2022.

[2] P. Kumar and R. Hasthantram, "Enabling zero-trust architecture using a federated learning framework with differential privacy and blockchain algorithms," *Proceedings of the 2024 4th International Conference on Mobile Networks and Wireless Communications (ICMNWC)*, pp. 1–6, 2024.

[3] J. Xiao, H. Nie, Z. Yi, and X. Tang, "Federated learning with bilateral defense via blockchain," *Neural Networks*, vol. 185, no. 3–4, p. 107199, 2025.

[4] L. Tran, S. Chari, M. S. I. Khan, A. Zachariah, S. Patterson, and O. Seneviratne, "A differentially private blockchain-based approach for vertical federated learning," *arXiv preprint arXiv:2407.07054*, 2024.

[5] Y. Li, C. Xia, W. Lin, and T. Wang, "Ppbfl: A privacy protected blockchain-based federated learning model," *arXiv preprint arXiv:2401.01204*, 2024.

[6] Z. Zhang, J. Jia, X. Cao, and N. Z. Gong, "Robust zero trust architecture: Joint blockchain based federated learning and anomaly detection based framework," *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, pp. 1–15, 2024.

[7] Y. Li, C. Xia, W. Lin, and T. Wang, "Ppbfl: A privacy protected blockchain-based federated learning model," *arXiv preprint arXiv:2401.01204*, 2024.

[8] T. Rückel, J. Sedlmeir, and P. Hofmann, "Fairness, integrity, and privacy in a scalable blockchain-based federated learning system," *arXiv preprint arXiv:2111.06290*, 2021.

[9] C. Zhang, H. Sun, Z. Shen, and D. Wang, "Cs-fl: Cross-zone secure federated learning with blockchain and a credibility mechanism," *Applied Sciences*, vol. 15, no. 1, p. 26, 2025.

[10] V. Mugunthan, R. Rahman, and L. Kagal, "Blockflow: An accountable and privacy-preserving solution for federated learning," *arXiv preprint arXiv:2007.03856*, 2020.

[11] Y. Li, C. Xia, W. Lin, and T. Wang, "Ppbfl: A privacy protected blockchain-based federated learning model," *arXiv preprint arXiv:2401.01204*, 2024.

[12] T. Rückel, J. Sedlmeir, and P. Hofmann, "Fairness, integrity, and privacy in a scalable blockchain-based federated learning system," *arXiv preprint arXiv:2111.06290*, 2021.

[13] E. Bandara, X. Liang, S. Shetty, R. Mukkamala, A. Rahman, and N. W. Keong, "Skunk — a blockchain and zero trust security enabled federated learning platform for 5g/6g network slicing," *Proceedings of the 2022 19th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, pp. 1–9, 2022.

[14] M. García-Márquez, N. Rodríguez-Barroso, M. V. Luzón, and F. Herrera, "Krum federated chain (kfc): Using blockchain to defend against adversarial attacks in federated learning," *arXiv preprint arXiv:2502.06917*, 2025.

[15] F. Ayaz, Z. Sheng, D. Tian, and Y. L. Guan, "A blockchain based federated learning for message dissemination in vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 71, pp. 1927–1940, 2022.

[16] B. Guo, "Privacy-preserving approach to edge federated learning based on blockchain and fully homomorphic encryption," *IEEE Dataport*, 2024.

[17] D. Commey, S. Hounsinou, and G. V. Crosby, "Securing health data on the blockchain: A differential privacy and federated learning framework," *arXiv preprint arXiv:2405.11580*, 2024.

[18] L. Tran, S. Chari, M. S. I. Khan, A. Zachariah, S. Patterson, and O. Seneviratne, "A differentially private blockchain-based approach for vertical federated learning," *arXiv preprint arXiv:2407.07054*, 2024.

[19] Y. Li, C. Xia, W. Lin, and T. Wang, "Ppbfl: A privacy protected blockchain-based federated learning model," *arXiv preprint arXiv:2401.01204*, 2024.