Gachi Whitepaper

Audum Labs

November, 2024

Abstract

Federated Learning (FL) enables collaborative model training without sharing raw data, preserving privacy across entities. Gachi enhances traditional FL by integrating Secure Multi-Party Computation (SMPC) for secure gradient aggregation, preventing data reconstruction at all stages.

Gachi's core innovation lies in its decentralized governance and tokenomics framework, using SubDAOs to incentivize high-quality data contributions and ensure accountability. Token-based incentives align participant contributions with ecosystem success. With SMPC, end-users can pay per inference for FL models, eliminating the need to purchase the entire model.

By combining SMPC, DAOs, and tokenomics, Gachi offers a scalable, privacy-preserving solution for decentralized AI development.

1 Introduction

1.1 Federated Learning in Privacy-Enhancing Technologies

The rapid advancement of artificial intelligence (AI) is driven by access to extensive datasets, but privacy concerns and regulatory restrictions often keep data siloed across organizations, hindering collaboration. Privacy-Enhancing Technologies (PETs) aim to address this challenge, and Federated Learning (FL) has emerged as a key PET for collaborative model training without compromising data privacy. FL allows multiple parties to train a shared global model by exchanging model updates instead of raw data, ensuring that sensitive information remains local.

Compared to other PETs like Fully Homomorphic Encryption (FHE) and Differential Privacy (DP), FL offers a more practical and efficient solution. While FHE is computationally expensive and DP can reduce model accuracy, FL combined with Secure Multi-Party Computation (SMPC) provides effective privacy protection and decentralized model training. Gachi builds on these principles by integrating SMPC for secure gradient aggregation, ensuring that individual participants' gradients remain confidential even during the collaborative update process, making it a scalable solution for privacy-preserving collaborative learning.

1.2 The Need for Incentivized Federated Learning and Governance

Despite its advantages, traditional FL systems face challenges in participant engagement and data quality. Without proper incentives, organizations may be reluctant to contribute their data or computational resources, leading to suboptimal model performance. Additionally, there's a risk of participants providing low-quality or even malicious data, which can corrupt the global model.

An incentivized FL platform with a robust governance structure is essential to address these challenges. By introducing token-based incentives and decentralized governance through SubDAOs (Sub Decentralized Autonomous Organizations), participants are motivated to contribute high-quality data and actively engage in the training process. External validators or peer reviewers are rewarded with tokens for ensuring the integrity and accuracy of model updates. This governance model not only fosters collaboration and trust among participants but also enhances the overall performance and reliability of the federated learning system.

2 Gachi Pipeline Overview

The Gachi pipeline is structured into multiple stages, each designed to ensure privacy, security, and effective participant incentives. Below is an overview of the entire process from training to inference:

1. **Local Training**: Each organization trains its model locally on private data, ensuring plaintext data never leaves the premise. SMPC is used to secret-share gradients, maintaining data confidentiality.

2. **Peer Validation**: Participants validate each other's model updates using secure 2PC (Garbled Circuits) to ensure data quality. External validators rank contributions, with top-ranked participants receiving higher rewards, motivating high-quality data sharing.

3. **Secure Gradient Aggregation**: Gradients are securely aggregated using SMPC. This ensures that no individual gradient is exposed during aggregation, and all computations occur on encrypted data.

4. **Global Model Update**: The aggregated gradients are used to update the global model. Governance tokens allow participants to vote on model updates, fostering transparency and community-driven decision-making.

5. **Token Incentives and SubDAO Governance**: Participants receive platform tokens as rewards, while SubDAO-specific governance tokens are distributed to contributors. These governance tokens are soul-bound, tied to active contributions, and revoked upon exit; for internal use only.

6. **Secure Inference**: The updated global model is available for inference. The model itself remains hidden from all participants. Input data from

end users is secret-shared using PETs, ensuring data privacy. Inference is performed on encrypted inputs, and results are securely returned to users.

7. **Pay-per-inference**: The inference process follows a pay-per-inference model, where users pay in platform tokens for each inference request. These are instantly distributed among contributors of the SubDAO in proportion to their ranking as previously determined during the peer validation phase.

8. **Lifecycle and Redistribution**: At the end of each federated learning cycle, SubDAO governance tokens are redistributed based on new contributions, ensuring ongoing engagement and sustainability.

3 Federated Learning

Federated Learning (FL) is a decentralized approach to machine learning where multiple clients collaboratively train a model without sharing their raw data. This preserves privacy, as data remains on each client device, and only model updates are shared with a central server for aggregation [1]. The goal is to minimize privacy risks while enabling the collective use of distributed data for model improvement [4].

3.1 Model Training in Federated Learning

In a typical federated learning setting, there are K clients, each holding a local dataset $\mathcal{D}_k = \{(x_i, y_i)\}_{i=1}^{n_k}$, where x_i represents the input features and y_i represents the corresponding labels. Each client aims to collaboratively train a global model $w \in \mathbb{R}^d$ (with d being the dimension of the model's parameters) without sharing their private dataset [2].

Each client k solves the following optimization problem locally:

$$\min_w F_k(w) = \frac{1}{n_k} \sum_{i=1}^{n_k} \ell(w; x_i, y_i)$$

where $\ell(w; x_i, y_i)$ is the loss function for the model w on the data point (x_i, y_i), and n_k is the number of data points at client k [3]. The global objective is to minimize the weighted average of these local objectives:

$$\min_w F(w) = \sum_{k=1}^{K} \frac{n_k}{n} F_k(w)$$

where $n = \sum_{k=1}^{K} n_k$ is the total number of data points across all clients [1].

3.2 Federated Averaging Algorithm

The most common algorithm used in federated learning is Federated Averaging (FedAvg) [1]. This algorithm works as follows:

1. Each client k initializes the model parameters $w_k^{(0)}$. 2. In each communication round t, the server sends the current global model $w^{(t)}$ to all clients. 3. Each client updates the model locally by solving the optimization problem using gradient descent or another optimization method:

$$w_k^{(t+1)} = w_k^{(t)} - \eta \nabla F_k(w_k^{(t)})$$

where η is the learning rate and $\nabla F_k(w_k^{(t)})$ is the gradient of the local loss function [3].

4. After the local updates, each client sends its updated model parameters $w_k^{(t+1)}$ back to the central server. 5. The server aggregates the updates from the clients to form the new global model:

$$w^{(t+1)} = \sum_{k=1}^{K} \frac{n_k}{n} w_k^{(t+1)}$$

This process is repeated for several rounds until the global model converges [1].

3.3 Privacy in Federated Learning

One of the core motivations behind federated learning is to ensure that data privacy is maintained. Unlike traditional machine learning approaches where data is centralized, federated learning keeps the data decentralized and only transmits model updates. However, the model updates themselves can still leak information about the underlying data (gradient leakage), leading to the need for additional privacy-preserving mechanisms, such as secure multi-party computation (SMPC), as will be explained below.

4 Platform-wide Blind Computing Solution

The in-house blockchain SMPC solution is integrated into the Gachi platform to enhance the efficiency, scalability, and security of federated learning. In this section, we outline how SMPC is used in our federated learning pipeline, providing detailed descriptions of each stage of the process.

4.1 Federated Learning Pipeline with SMPC

4.1.1 Model Training On-Premise

Each member trains a local model on its private data using on-premise hardware resources such as GPU clusters. After the local training phase, each member obtains gradients, which must remain confidential to prevent gradient leakage. Instead of sharing these raw gradients, SMPC is used to securely share and aggregate these values [4].

4.1.2 Pairwise Peer Validation Using 2PC (Garbled Circuits)

After training, each member's weights are validated externally with each other's data using a Two-Party Computation (2PC) approach. Specifically, the Garbled Circuits protocol is used to ensure pairwise peer validation while keeping both the model weights and the input data confidential.

Let w_i be the weights from member i and x_j be the data from member j. In 2PC, member i and member j collaborate to validate w_i against x_j without revealing their respective data. The process involves the following steps:

1. Member i creates a garbled circuit that represents the validation function $f(w_i, x_j)$, which evaluates the model weights against the peer's data. 2. Member j receives the garbled circuit and encrypted input labels, which they use to evaluate the function without learning anything about w_i. 3. The output of the function is shared between both members to confirm the validation result without revealing any underlying data.

The garbled circuit ensures that neither w_i nor x_j is disclosed during the validation process. This approach allows each member to validate the accuracy and reliability of another member's model weights while maintaining complete data confidentiality [7].

Mathematically, let $f(w_i, x_j)$ represent the validation function. The result y_{ij} of the pairwise validation is computed as:

$$y_{ij} = f(w_i, x_j),$$

where $f(\cdot)$ is computed using garbled circuits to maintain privacy. This ensures that each pairwise validation step is secure and does not expose any sensitive information.

4.1.3 Secure Gradient Aggregation

The decentralized nodes perform secure multi-party computation to aggregate the validated gradients from all participating members. The aggregation is carried out in a non-interactive manner, reducing communication overhead while maintaining data privacy [7]. Specifically, each node performs computations on the shares it possesses, and the aggregated gradients G_{agg} are computed as:

$$G_{agg} = \sum_{i=1}^{K} w_i,$$

where K is the number of participating members. This method ensures that none of the nodes or members can reconstruct the original gradients, as only the final aggregated gradients are securely output [8].

4.1.4 Securing Final Aggregated Gradients

The final aggregated gradients are kept secure using the SMPC protocol, ensuring that they remain inaccessible to unauthorized entities. These gradients are then used for inference, and access is provided only through privacy-preserving channels that prevent unauthorized viewing [9].

4.1.5 Inference Requests from End Users

When an end user, such as a patient's wearable device or a healthcare provider, requests an inference, the input data is secret-shared and masked using the preprocessing phase of the SMPC protocol. This ensures that the input data remains fully confidential throughout the inference process, with no party in the network, including nodes or members, having access to the unmasked input [10].

Let x be the input data from the end user. Using LSSS, x is split into n shares, $x_1, x_2, \ldots, x_n$, such that:

$$x = \sum_{j=1}^{n} \lambda_j x_j,$$

where λ_j are random coefficients. These shares are distributed across the nodes for secure inference.

4.1.6 Secure Inference Using SMPC

The secret-shared aggregated gradients and secret-shared input data are combined using SMPC. The decentralized network of nodes performs secure inference on the masked data using non-interactive SMPC, which eliminates the need for multiple communication rounds [11]. The inference result y is computed as:

$$y = f(G_{agg}, x),$$

where $f(\cdot)$ represents the inference function applied to the aggregated gradients and input data. This process ensures that inference is both fast and privacy-preserving [12].

4.1.7 Returning Inference Results

The inference results are returned to the requesting party in an encrypted or masked form. Only the intended recipient can decrypt and view the results, ensuring that neither the members nor the nodes have access to the final output. This guarantees that the entire process, from training to inference, remains private and secure [13].

4.2 Key Benefits of Using SMPC

- **Privacy-Preserving Validation and Secure Aggregation:** SMPC enables privacy-preserving peer validation and secure aggregation of gradients using protocols like 2PC and garbled circuits, ensuring that no single entity can access the complete data or model weights [7, 8].

- **Scalability and Efficiency:** The non-interactive nature of SMPC reduces communication overhead, making it highly scalable and efficient for large numbers of participants, suitable for large-scale federated learning scenarios [15, 18].
- **End-to-End Security and Confidential Inference:** SMPC ensures confidentiality of both input data and inference results, offering end-to-end protection against data leakage throughout the federated learning pipeline [10, 17].
- **Decentralization and Robustness:** The decentralized structure of the SMPC system, particularly in blockchain-based solutions, eliminates single points of failure and reduces the risks associated with centralized data breaches [16].

5 Third-party Blind Computing Solution

The third-party blockchain SMPC solution leverages Nillion's unique decentralized technology to enhance federated learning on the Gachi platform. Unlike the in-house blockchain-based SMPC approach, which relies on SubDAO-wide compute, Nillion's system relies on a broader, more decentralized architecture that removes the need for direct peer-to-peer interactions. This section highlights the key differences and advantages of using Nillion's public blockchain approach over the private solution [29].

5.1 Key Differences in Nillion's SMPC Implementation

5.1.1 Decentralized Node Architecture

Nillion's public blockchain spreads computation across a wide, decentralized network of nodes. This ensures that no single entity controls the flow of data or computations, improving privacy and removing single points of failure [29].

5.1.2 NMC for Data Splitting and Distribution

Nillion uses its proprietary Nil Message Compute (NMC) protocol, which securely splits data across nodes without requiring private or encrypted communication. This allows for faster and more scalable operations compared to traditional secret-sharing methods, which often involve higher communication overhead [29].

5.1.3 Trustless Validation and Aggregation

The validation and aggregation process in Nillion's system is conducted entirely by its decentralized network. Rather than relying on pairwise peer validation (e.g., garbled circuits or Two-Party Computation), Nillion's nodes handle the validation across the network, providing trustless and distributed peer validation. This allows for greater scalability and security without the need for complex, interactive protocols between federated learning members [29, 30].

5.1.4 Non-Interactive, Large-Scale Gradient Aggregation

While Blockchain solutions require interactive exchanges to aggregate gradients, Nillion's SMPC eliminates this requirement. Its non-interactive, trustless aggregation process ensures that gradients can be securely aggregated across a large number of participants without the need for direct communication between nodes or members. This improves scalability and reduces computational and communication overhead [31].

5.1.5 Decentralized Inference and Data Security

Inference requests are handled using Nillion's decentralized nodes, further enhancing privacy and security. No single party holds complete access to the data or the aggregated model. With many more nodes outside of the SubDAO, collusion among members is now rendered meaningless. The end-to-end decentralization makes the system inherently more resistant to breaches and data reconstruction attacks [29].

5.2 Key Benefits of Nillion

- **Higher Decentralization:** Computations are distributed across a larger network of nodes, improving security by removing central control or direct peer-to-peer interactions.
- **Scalable and Trustless Operations:** Nillion's infrastructure allows for non-interactive, trustless validation and aggregation, improving scalability without sacrificing privacy or efficiency.
- **No Private Communications:** The NMC technique avoids the need for encrypted channels, reducing communication costs while maintaining data confidentiality across a decentralized network.
- **Robust Against Single Points of Failure:** The system is more resilient to attacks and data breaches due to the full decentralization of both gradient aggregation and inference.
- **Efficient and Secure Inference:** By leveraging a distributed network for inference, Nillion ensures that inference remains fast, secure, and privacy-preserving, even for large-scale deployments.

6 Governance and Incentives Model

The governance model of Gachi has been designed to ensure decentralized, transparent, and effective decision-making across the federated learning ecosystem. The governance structure revolves around the use of the platform token as the core utility for governance, rewards, and transactions. This section provides an overview of the governance and incentives framework.

6.1 Platform Token Governance

The entire Gachi ecosystem is governed by the platform token, which serves as the foundation for governance decisions, rewards distribution, and payment for inference usage. The platform token ensures alignment of interests across the platform and provides a unified governance approach.

Key Governance Mechanisms:

- **Voting Rights:** Platform token holders participate in votes related to ecosystem-wide decisions. Proposals include adjusting fee rates for inference usage.
- **SubDAO Creation:** When a new SubDAO is created, participants invest platform tokens. In return, they receive soul-bound SubDAO governance tokens, which are non-transferable and revoked upon exiting the SubDAO [21].
- **Fee Rate Determination:** Platform token holders determine the fee rate for inference usage by non-SubDAO members, ensuring that value is accrued to the overall ecosystem.

6.2 Incentives and Reward Mechanism

The incentives within the Gachi ecosystem are designed to reward participants for their contributions to federated learning models, encouraging high-quality data contributions, model validation, and sustained engagement.

6.2.1 Platform Token Rewards

Participants contributing to SubDAOs—whether by providing data, computational resources, or validation—are rewarded in platform tokens. These rewards incentivize participants to contribute high-quality work, as the amount of reward is tied to the quality and significance of their contributions [24].

Reward Distribution:

- **Data and Compute Contributions:** Contributors providing data and compute resources in the form of uploading gradients are rewarded in proportion to the quality of their data (*i.e* model update) [25]. This quality is determined by the averaged metric posted by peer validators who "review" the model updates against their own data (securely using Nilliion).

- **Peer validation:** Peer validators are also rewarded for their compute per external validation performed. The amount rewarded is constant per validation as previously determined by the SubDAO in relation to the reward pool (*i.e* the SubDAO treasury created by the investment pool).

6.2.2 Inference Usage Payments

Inference usage is divided into two parts: SubDAO members and non-SubDAO members.

Inference for Third-parties:

- Non-SubDAO members must pay a price for inference, as determined by SubDAO or platform (SuperDAO). Out of each transaction, a cut is taken by the platform, with the fee rate determined by the SuperDAO [4].
- All inference payments are made using platform tokens, ensuring that value flows back into the ecosystem.

7 Use Case: Pharmaceutical Companies

Pharmaceutical companies can utilize the Gachi platform to develop advanced models derived from personal health records (PHR) data provided by individuals. These models can be applied to tasks such as market segmentation, treatment response prediction, or Health Economics and Outcomes Research (HEOR) analysis. This section provides an overview of how the Gachi ecosystem leverages individual contributions of PHR data to create real-world evidence (RWE) models.

7.1 Model Request by Pharma Company

A pharmaceutical company submits a request on the Gachi platform, specifying the need for a machine learning model to address a particular research or business objective. For example, the company may request:

- **Market Segmentation and Sizing Model**: A model to categorize patient populations based on specific clinical attributes and estimate the size of potential markets for a new drug.
- **Treatment Response Model**: A predictive model that identifies which subsets of patients are likely to respond positively to a specific treatment, using past outcomes and clinical characteristics.
- **HEOR Model**: A Health Economics and Outcomes Research model that evaluates the clinical and economic impacts of treatments, considering metrics such as quality-adjusted life years (QALYs) and healthcare costs.

The request includes specifications such as input data requirements, the intended use case, desired performance metrics (such as accuracy, sensitivity, and specificity), and a proposed budget for the model's development.

7.2 Participation by Individuals through Gachi

Individuals with relevant PHR data, such as medical histories, treatment outcomes, and clinical variables, can opt to participate by contributing their data through the Gachi platform. This data is used in a federated learning process, which ensures that individuals' sensitive information remains private. Data contributors retain full control over their information, as their personal data is never shared directly with the pharmaceutical company or any other third party.

7.3 Model Development Using the Gachi Pipeline

The model development process in Gachi is designed to protect data privacy and provide incentives for individual participants:

1. **Local Model Training**: Each individual's PHR data is used locally to train a machine learning model in accordance with the pharmaceutical company's specifications. The data remains private, and only model updates (such as gradients) are shared with the platform.

2. **Secure Gradient Aggregation**: Gradients from all participating individuals are securely aggregated using Secure Multi-Party Computation (SMPC) techniques, ensuring that no personal data is exposed. The aggregation produces an updated global model without any raw data being transferred.

3. **Global Model Update**: The aggregated gradients are used to iteratively improve the global model. The pharmaceutical company, as the model requester, can monitor model progress and provide feedback or request adjustments if needed.

4. **Incentives and Rewards**: Individuals are rewarded for contributing their PHR data, receiving platform tokens proportional to the quality of their data and the model's improvement. This ensures that contributors are fairly compensated for their role in model development.

7.4 Pay-per-Inference and Long-term Value

Instead of purchasing large anonymized datasets, pharmaceutical companies benefit from a pay-per-inference model. This allows them to pay only for the specific inferences they need, making the approach more cost-effective. Revenue generated from inference requests is distributed to individual contributors based on their contributions to the model, ensuring that participants receive ongoing compensation.

This pay-per-inference model supports continuous learning cycles as individuals update their PHR data. It ensures a steady flow of high-quality data for model improvements, fostering long-term collaboration between individuals and pharmaceutical companies, with continuous incentives for data contribution and model refinement.

References

[1] H. B. McMahan, E. Moore, D. Ramage, S. H. Y. Arcas, and K. M. R. et al., "Communication-Efficient Learning of Deep Networks from Decentralized Data," in *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*, 2017.

[2] K. Bonawitz, V. Rastogi, E. Shelat, et al., "Towards Federated Learning at Scale: System Design," in *Proceedings of the 2nd SysML Conference*, 2019.

[3] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated Machine Learning: Opportunities and Challenges," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 30, no. 2, pp. 502-516, 2019.

[4] Kairouz, P., et al. "Advances and Open Problems in Federated Learning." *arXiv preprint arXiv:1912.04977*, 2019.

[5] Shamir, A. "How to share a secret." *Communications of the ACM*, vol. 22, no. 11, 1979, pp. 612-613.

[6] Benaloh, J. "Secret sharing homomorphisms: Keeping shares of a secret secret." *EUROCRYPT*, 1996, pp. 251-260.

[7] Yao, A. C. "How to generate and exchange secrets." *Foundations of Computer Science*, 1986, pp. 162-167.

[8] Goldreich, O. "Secure multi-party computation." *Manuscript. Preliminary version*, 1998.

[9] Rivest, R. L., et al. "A method for obtaining digital signatures and public-key cryptosystems." *Communications of the ACM*, vol. 21, no. 2, 1978, pp. 120-126.

[10] Damgård, I., et al. "Multiparty computation from somewhat homomorphic encryption." *Advances in Cryptology–CRYPTO*, 2012, pp. 643-662.

[11] Evans, D., et al. "Pragmatic privacy preserving computation." *Proceedings on Privacy Enhancing Technologies*, vol. 2018, no. 1, 2018, pp. 1-24.

[12] Keller, M. "MP-SPDZ: A versatile framework for multi-party computation." *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, 2020, pp. 1575-1590.

[13] Gentry, C. "Fully homomorphic encryption using ideal lattices." *STOC*, 2009, pp. 169-178.

[14] Grover, L. K. "A fast quantum mechanical algorithm for database search." *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, 1996, pp. 212-219.

[15] Ben-Or, M., et al. "Completeness theorems for non-cryptographic fault-tolerant distributed computation." *Proceedings of the twentieth annual ACM symposium on Theory of computing*, 1988, pp. 1-10.

[16] Chaum, D. "The dining cryptographers problem: Unconditional sender and recipient untraceability." *Journal of Cryptology*, vol. 1, no. 1, 1988, pp. 65-75.

[17] Goldwasser, S., and Micali, S. "Probabilistic encryption." *Journal of Computer and System Sciences*, vol. 28, no. 2, 1982, pp. 270-299.

[18] Boyd, C., et al. "Efficient Secure Computation with Minimal Interaction." *IEEE Transactions on Information Forensics and Security*, vol. 16, 2021, pp. 2468-2480.

[19] Buterin, V. "Decentralized Governance for Blockchain Ecosystems." *Ethereum Blog*, 2021.

[20] Zheng, Z., et al. "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends." *IEEE International Congress on Big Data*, 2017.

[21] Nguyen, Q. K. "Blockchain: A Game Changer for Decentralized Applications." *Journal of Computers*, vol. 9, no. 2, 2020, pp. 45-50.

[22] Chen, M., et al. "Privacy-Preserving Federated Learning for Medical Imaging." *Nature Machine Intelligence*, 2021.

[23] Nakamoto, S. "Bitcoin: A Peer-to-Peer Electronic Cash System." 2008.

[24] Hardy, S., et al. "Private Federated Learning on Vertically Partitioned Data via Entity Resolution and Additively Homomorphic Encryption." *IEEE Transactions on Information Forensics and Security*, 2019.

[25] Yang, Q., et al. "Federated Machine Learning: Concept and Applications." *ACM Transactions on Intelligent Systems and Technology*, 2019.

[26] Rieke, N., et al. "The Future of Digital Health with Federated Learning." *NPJ Digital Medicine*, 2020.

[27] Truex, S., et al. "A Hybrid Approach to Privacy-Preserving Federated Learning." *Proceedings of the 2019 ACM Conference on Data and Application Security and Privacy*, 2019.

[28] Xu, J., et al. "Federated Learning for Healthcare Informatics." *Journal of Healthcare Informatics Research*, 2020.

[29] Nillion. Nillion Builder Docs. Nillion Documentation, 2023. Available at: https://docs.nillion.com/

[30] Zhao, C., Zhao, S., Zhao, M., Chen, Z., Gao, C., Li, H., Tan, Y. Secure multi-party computation: Theory, practice, and applications. Information Sciences, 476, 357-372, 2019.

[31] Yu, S., Cui, L. Secure Multi-party Computation in Federated Learning. In: Security and Privacy in Federated Learning. Springer, Singapore, 2023.