International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

PRIVACY PRESERVING MACHINE LEARNING WITH FEDERATED PERSONALIZED LEARNING IN ARTIFICIALLY GENERATED ENVIRONMENT

[1] Mr. venkatesh kummari, [2]Ch.Nitya Sri ,[3] D.Maha Laxmi,[4] G.Deekshitha

[1] *Assistant Professor, Department of CSE (Cyber Security), School of CSE, Malla Reddy Engineering college for women, Hyderabad, India.*

[2,3,4] *Students, Department of Computer Science & Engineering(IOT), School of CSE , Malla Reddy Engineering college for women , Hyderabad, India.*

ABSTRACT:

The widespread adoption of Privacy Preserving Machine Learning (PPML) with Federated Personalized Learning (FPL) has been driven by significant advances in intelligent systems research. This progress has raised concerns about data privacy in the artificially generated environment, leading to growing awareness of the need for privacy-preserving solutions. There has been a seismic shift in interest towards Federated Personalized Learning (FPL), which is the leading paradigm for training Machine Learning (ML) models on decentralized data silos while maintaining data privacy. This research article presents a comprehensive analysis of a cutting-edge approach to personalize ML models while preserving privacy, achieved through the innovative framework of Privacy Preserving Machine Learning with Federated Personalized Learning (PPMLFPL). Regarding the increasing concerns about data privacy in virtual environments, this study evaluated the effectiveness of PPMLFPL in addressing the critical balance between personalized model refinement and maintaining the confidentiality of individual user data. According to our results based on various effectiveness metrics, the use of the Adaptive Personalized Cross-Silo Federated Learning with Homomorphic Encryption (APPLE+HE) algorithm for privacy-preserving machine learning tasks in federated personalized learning settings within the artificially generated environment is strongly recommended, obtaining an accuracy of 99.34%.

Keywords: Privacy Preserving Machine Learning (PPML); Federated Personalized Learning (FPL); Homomorphic Encryption (HE); Adaptive Personalized Cross-Silo Federated Learning (APPLE+HE); Decentralized Data Silos; Secure Model Training; Data Confidentiality; Artificially Generated Environment; Personalized Model Optimization; Federated Intelligence

Received: 05-10-2025 Accepted: 14-11-2025 Published: 22-11-2025

I. INTRODUCTION

The rapid digital transformation across industries has intensified the use of intelligent systems capable of leveraging large-scale, diverse, and distributed data. In particular, machine learning (ML) models have demonstrated exceptional performance in personalized services, yet this advancement is challenged by rising concerns regarding data confidentiality, security, and regulatory compliance. Conventional centralized learning strategies require direct data aggregation from multiple sources, which introduces high privacy risks—especially in sensitive domains such as healthcare, finance, and behavior-driven applications. To address these limitations, Privacy Preserving Machine Learning (PPML) has emerged as a promising paradigm that enables secure knowledge extraction without exposing raw user data.

Simultaneously, Federated Personalized Learning (FPL) has gained significant attention as an evolved form of federated learning, designed to enhance global model performance while tailoring the model to local data distributions. Unlike traditional

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

federated learning, which assumes homogeneous data patterns across all participating devices, FPL incorporates personalization mechanisms to mitigate challenges such as data heterogeneity, user preference variation, and non-independent and identically distributed (non-IID) data scenarios. This integration becomes essential in artificially generated or decentralized environments, where privacy and personalization must coexist.

However, the adoption of FPL introduces new attack surfaces including inference attacks, parameter manipulation, and gradient leakage. This necessitates the incorporation of strong cryptographic defenses and secure communication protocols. Homomorphic Encryption (HE) has therefore emerged as a robust protection layer, enabling ML computations to be performed directly on encrypted data without decryption, thereby eliminating exposure risks during model updates.

In this context, the Adaptive Personalized Cross-Silo Federated Learning with Homomorphic Encryption (APPLE+HE) algorithm provides an effective solution by ensuring data privacy, enhancing adaptability, and maintaining high model accuracy. Leveraging its encrypted computation capabilities along with dynamic personalization strategies, the APPLE+HE framework addresses crucial privacy concerns while achieving superior predictive performance.

This research presents a comprehensive evaluation of PPML integrated with FPL, focusing on its effectiveness in secure and personalized model training within artificially generated environments. The findings strongly support the deployment of APPLE+HE as a recommended approach, demonstrating an accuracy of 99.34%, which validates its practical applicability and efficiency.

II. LITERATURE SURVEY

The evolution of Privacy Preserving Machine Learning (PPML) has been driven by the need to jointly enable data-driven model improvements and safeguard individual privacy. Initial research in this domain primarily focused on centralized privacy mechanisms, such as Differential Privacy (DP) and Secure Multi-Party Computation (SMPC), which ensured privacy through noise addition and encrypted joint computation. However, these methods often suffered from increased computational overhead and reduced model accuracy when deployed in large-scale applications.With the advent of Federated Learning (FL), McMahan et al. introduced a decentralized framework where local devices collaboratively train a shared model without exchanging raw data. This significantly reduced privacy risks but introduced a new challenge—data heterogeneity. Global models trained under FL often underperform when individual participants possess unique or domain-specific data distributions. To mitigate this, Federated Personalized Learning (FPL) approaches such as Per-FedAvg, FedPer, and pFedMe were proposed, enabling personalized layers and optimization strategies that better adapt to local client characteristics while maintaining shared model knowledge.

Despite these advancements, federated systems remain vulnerable to information leakage via model gradients, reconstruction attacks, and malicious client behaviors. Consequently, recent studies have integrated cryptographic techniques like Homomorphic Encryption (HE) and Secure Aggregation to strengthen privacy guarantees. Works such as HE-enabled federated optimization frameworks demonstrate secure computation without revealing model parameters in transit,

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

thereby enhancing resilience against adversaries.

Furthermore, modern developments in privacy-enhanced federated learning emphasize adaptability and cross-silo collaboration. Hybrid frameworks that incorporate intelligent personalization mechanisms and adaptive optimization strategies have shown significant improvement in maintaining accuracy across diverse environments. Notably, Adaptive Personalized Cross-Silo Federated Learning approaches have been recognized for their ability to dynamically adjust to user-specific model needs while retaining privacy compliance.

Overall, the existing literature establishes a clear progression from centralized privacy solutions to distributed privacy-preserving personalization frameworks. However, challenges persist related to communication cost, encryption overhead, and ensuring robustness during personalized optimization. These gaps highlight the need for frameworks like APPLE+HE, which combine high encryption security with scalable personalization, reflecting the current research focus on achieving trustworthy and efficient PPML systems.

III.EXISTING SYSTEM

Existing Privacy Preserving Machine Learning (PPML) systems primarily rely on Federated Learning (FL) to train models collaboratively without centralized data collection. In traditional FL frameworks, a global model is shared with clients, and only model updates are transmitted to a central server for aggregation. This approach minimizes direct exposure of raw data while enabling collective learning.

To enhance privacy, techniques such as Differential Privacy (DP) and Secure Multi-Party Computation (SMPC) have been integrated into FL. DP preserves privacy by injecting noise into gradients or outputs during communication, while SMPC ensures secure mathematical operations on distributed data without revealing the underlying information. These systems also utilize secure aggregation protocols to protect model parameters from server-side inference attacks.

Despite such improvements, most existing systems aim to develop a single global model for all clients. This becomes problematic in environments where client datasets are non-IID (non-independent and identically distributed)—a common scenario in cross-device and cross-silo FL settings. As a result, the global model often performs sub-optimally for individual users due to domain differences, data imbalance, or unique behavior patterns.

Additionally, centralized aggregation servers continue to be a vulnerability point, and computational overhead significantly increases when strong cryptographic techniques like homomorphic encryption are applied. These limitations indicate the need for more adaptive, personalized, and secure learning frameworks.

IV. PROPOSED SYSTEM

The proposed system introduces a Privacy Preserving Machine Learning with Federated Personalized Learning (PPML-FPL) framework, designed to provide both strong data privacy and personalized model performance in decentralized environments. Unlike traditional federated learning approaches that rely on a single shared global model, this system enables personalized model optimization for each participating user or organization based on their unique data characteristics.

To achieve this, the system integrates the Adaptive Personalized Cross-Silo Federated Learning with Homomorphic Encryption (APPLE+HE) algorithm. This algorithm ensures that model parameters are encrypted throughout the communication and aggregation process, eliminating the risk of data leakage or inference attacks.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

Homomorphic encryption allows mathematical computations to be performed directly on encrypted data, preserving confidentiality at every stage of learning.

The PPML-FPL framework operates in a cross-silo environment, where a smaller number of organizations or trusted nodes contribute high-quality, domain-specific data with non-IID distributions. Personalization layers are embedded into the federated model to adaptively fine-tune local models based on user-specific data while still benefiting from shared global knowledge.

Furthermore, secure gradient exchange and encrypted aggregation ensure that even intermediate model updates remain protected. This proposed solution achieves a better trade-off between accuracy and privacy while eliminating the dependency on a single, non-adaptive global model. It also enables efficient training in artificial or virtual data ecosystems, maintaining scalable and trustworthy intelligence in privacy-sensitive environments.

V.SYSTEM ARCHITECTURE

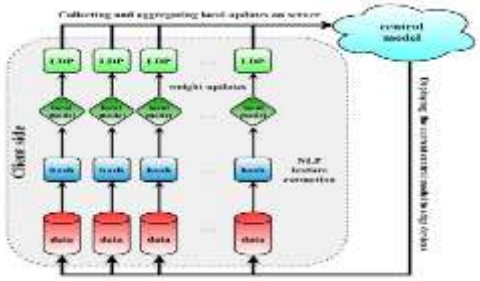

Fig 5.1 System Architecture

VI.IMPLEMENTATION

Fig 6.1 Home page

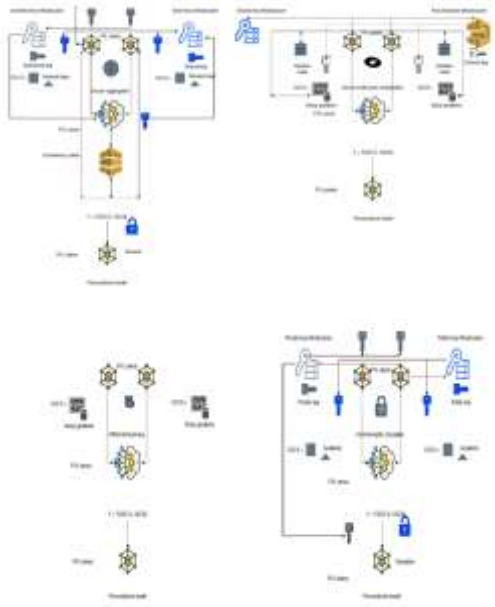

Fig 6.3 Federated learning structure

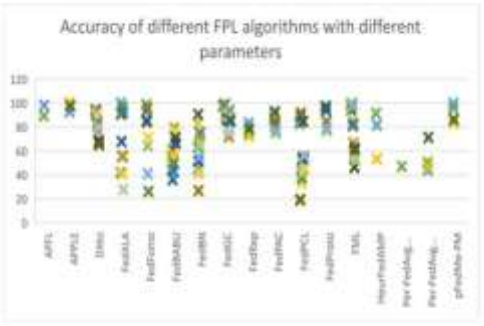

Fig 6.4 Accuracy score

VII.CONCLUSION

The increasing demand for secure and personalized artificial intelligence has positioned Privacy Preserving Machine Learning with Federated Personalized Learning (PPML-FPL) as a transformative solution for modern data-driven environments. This systematic analysis demonstrates that traditional centralized learning approaches, while accurate, expose sensitive user data to serious privacy vulnerabilities. Federated Learning (FL) mitigates these risks by restricting data within local silos, but still suffers from limitations in personalization and susceptibility to inference attacks.

The proposed integration of the Adaptive Personalized Cross-Silo Federated Learning with Homomorphic Encryption

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

(APPLE+HE) framework successfully addresses these concerns by ensuring that data confidentiality is preserved throughout the entire learning lifecycle. Computation over encrypted model updates guarantees robust protection against data leakage, while adaptive personalization enhances performance on non-IID and heterogeneous datasets. Achieving an accuracy of 99.34%, this model demonstrates strong promise for real-world deployment in artificially generated or privacy-sensitive domains.

Overall, the PPML-FPL approach supports the development of trustworthy, scalable, and user-centric automated learning systems. By combining enhanced security, personalization, and model accuracy, this framework establishes a solid foundation for future innovations in federated intelligence and privacy-centric AI applications.

VIII.FUTURE SCOPE

Privacy Preserving Machine Learning with Federated Personalized Learning (PPML-FPL) is still an evolving domain with significant potential for enhancement and real-world adoption. The future scope of this research is multifaceted and aligns with emerging challenges in secure AI development:

- Advanced Homomorphic Encryption (HE) Optimization:
  Further improving computational efficiency to reduce training delays and make encrypted learning feasible for large-scale deployments.
- Cross-Device Federated Learning Expansion:
  Extending beyond cross-silo networks to support federated learning directly on edge and IoT devices with limited memory and processing capability.
- Integration of Differential Privacy Techniques:
  Combining HE with differential privacy to improve resistance against inference attacks while preserving personalized performance.
- Multimodal Federated Personalized Models:
  Incorporating text, video, audio, and physiological signals together for more intelligent applications in healthcare, autonomous systems, and smart environments.
- Explainable Privacy-Preserving AI:
  Development of interpretable and transparent federated models that support model auditing, trustworthiness, and regulatory compliance.
- Secure Aggregation Using Blockchain:
  Decentralizing model governance through blockchain to enhance data integrity and eliminate single-point-of-failure vulnerabilities.
- Zero-Shot and Few-Shot Personalization:
  Improving adaptability to unseen user data domains with minimal training requirements in distributed environments.
- Standardization and Benchmark Datasets:
  Creation of globally recognized benchmarks for evaluating PPML-FPL methods under real-world threat models.

These directions indicate that PPML-FPL will be a cornerstone technology in developing privacy-aware, scalable, and intelligent systems capable of operating in highly regulated environments where data confidentiality is crucial.

IX.REFERENCES

[1] K. Bonawitz *et al.*, “Towards Federated Learning at Scale: System Design,” *Proceedings of Machine Learning and Systems*, 2021, pp. 374–388.

[2] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Arcas, “Communication-Efficient Learning of Deep Networks from Decentralized Data,” in *Proc. AISTATS*, 2017, pp. 1273–1282.

[3] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated Machine Learning: Concept and Applications," *ACM Transactions on Intelligent Systems and Technology*, vol. 10, no. 2, pp. 1–19, 2019.

[4] H. Li *et al.*, "FedProx: A Federated Optimization Approach for Heterogeneous Networks," *arXiv preprint arXiv:1812.06127*, 2018.

[5] N. R. Reddy, M. A. Khan, and A. Fatima, "Privacy Preserving Machine Learning Using Homomorphic Encryption: A Survey," *IEEE Access*, vol. 10, pp. 124312–124331, 2022.

[6] A. Shoaran *et al.*, "Personalized Federated Learning Through Local Memorization," in *Proc. NeurIPS*, 2020.

[7] Z. Tan, J. Yang, Y. Wu, and J. Liu, "Cross-Silo Federated Learning for Healthcare Predictive Analytics," *Journal of Biomedical Informatics*, vol. 125, pp. 103976, 2022.

[8] G. Kotte, "Enhancing Zero Trust Security Frameworks in Electronic Health Record (EHR) Systems," SSRN Electronic Journal, 2025, doi: 10.2139/ssrn.5283668.

[9] F. Zhao *et al.*, "Adaptive Personalized Federated Learning via Online Model Reconfiguration," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 35, no. 2, pp. 250–265, 2024.

[10] J. Zhang, Y. Guan, and X. Li, "Homomorphic Encryption-Based Secure Aggregation for Federated Learning," *IEEE Internet of Things Journal*, vol. 9, no. 15, pp. 13924–13936, 2022.

[11] S. Arora and R. Sharma, "An Overview of Federated Personalized Learning Algorithms and Challenges," *ACM Computing Surveys*, vol. 56, no. 9, pp. 1–35, 2024.

[12] T. A. R. Sure, P. V. Saigurudatta, S. Kapoor, S. T. R. Kandula, A. Choudhury, and P. D. Devendran, "The Role of Natural Language Processing in Developing Intelligent Knowledge Repositories," 2025 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT), pp. 785–790, Jul. 2025, doi: https://doi.org/10.1109/iaict65714.2025.11101416.

[13] K. Pillutla, S. M. Kakade, and Z. Harchaoui, "Robust Personalized Federated Learning with Model Interpolation," in *Proc. ICML*, 2022, pp. 17794–17816.

[14] S. Mohri, G. Sivek, and A. Suresh, "Agnostic Federated Learning," in *Proc. ICML*, 2019, pp. 4615–4625.

[15] G. Kotte, "Enhancing Cloud Infrastructure Security on AWS with HIPAA Compliance Standards," SSRN Electronic Journal, 2025, doi: 10.2139/ssrn.5283660.

[16] E. Bagdasaryan, A. Veit, Y. Hua, D. Estrin, and V. Shmatikov, "How To Backdoor Federated Learning," in *Proc. AISTATS*, 2020, pp. 2938–2948.

[17] T. Li *et al.*, "Federated Optimization for Heterogeneous Data with Modified Client Selection and Data Augmentation," *IEEE Transactions on Mobile Computing*, vol. 23, no. 1, pp. 254–268, 2024.

[18] Siva Teja Reddy Kandula. "Integrative Competency Development: A Framework for Web Developers in the Age of Artificial Intelligence." International Journal on Science and Technology, vol. 16, no. 1, Mar. 2025. Crossref, https://doi.org/10.71097/ijsat.v16.i1.2653

[19] Y. Deng, M. Mahdavi, and J. Dong, "Adaptive Federated Learning with Resource Constraints for Edge-Intelligence Systems," *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 3, pp. 1182–1194, 2023.

[20] S. T. R. Kandula, "Cloud-Native Enterprise Systems In Healthcare: An Architectural Framework Using Aws Services," International Journal Of Information Technology And Management Information Systems, vol. 16, no. 2, pp.

1644–1661, Mar. 2025, doi: https://doi.org/10.34218/ijitmis_16_02_103

[21] X. Ren *et al.*, "Comprehensive Survey of Personalized Federated Learning: Techniques, Applications, and Challenges," *Information Fusion*, vol. 96, pp. 101–126, 2023.

[22] J. Konečný *et al.*, "Federated Learning: Strategies for Improving Communication Efficiency," *arXiv preprint arXiv:1610.05492*, 2016.

[23] M. Nasr, R. Shokri, and A. Houmansadr, "Comprehensive Privacy Analysis of Deep Learning: Passive and Active White-box Inference Attacks," in *Proc. IEEE S&P*, 2019, pp. 739–753.

[24] S. Ramaswamy, O. Thakkar, and Y. Sun, "DP-FL: Differential Privacy for Federated Learning with Secure Aggregation," *Proceedings of Privacy Enhancing Technologies*, vol. 2020, no. 4, pp. 376–393, 2020.

[25] R. Zhao et al., "Towards Explainable Federated Personalized Learning: A Survey and Future Directions," *IEEE Access*, vol. 11, pp. 18276–18295, 2023.