www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

SECURE DECENTRALIZED AGGREGATION FOR PRIVACY PROTECTION IN EDGE-BASED FEDERATED LEARNING

Dr.M.VINAYA BABU[1], J.KARTHIK[2], K.ANUSRI[3], K.TEJASWINI[4]

[1]Associate Professor, Department of Computer Science and Engineering, Teegala Krishna Reddy Engineering College(An Autonomous Institution), Medbowli, Meerpet, Saroornagar, Hyderabad-500097

[2,3,4,]Students, Department of Computer Science and Engineering, Teegala Krishna Reddy Engineering College(An Autonomous Institution), Medbowli, Meerpet, Saroornagar, Hyderabad-500097

ABSTARCT

Federated Learning (FL) is a machine learning approach enabling multiple users to collaboratively train a global model by sharing their local models while preserving data privacy by avoiding raw data exchange. However, frequent parameter sharing between users and the aggregator increases the risk of membership privacy leakage. To address this, we propose LiPFed, a computationally lightweight and privacy-preserving FL scheme for edge networks, leveraging secure decentralized aggregation. By incorporating blockchain technology and an additive secret-sharing algorithm, LiPFed ensures the privacy of both local and global models while protecting against potential aggregator compromises. A smart contract is introduced to detect malicious models from edge nodes, ensuring only trustworthy global models are shared with users. Rigorous security analysis confirms its privacy-preserving capabilities, and extensive experiments demonstrate LiPFed's superiority over state-of-the-art schemes in training efficiency, model accuracy, and privacy protection.

I.INTRODUCTION

As a result of the advancement of artificial intelligence (AI) and machine learning (ML), issues related to data privacy and safety have become focal points of concern. Traditional centralized machine learning systems require the accumulation of user data into a singular repository which raises serious privacy and safety concerns. To tackle these issues, Federated Learning (FL) has emerged as a popular decentralized paradigm where models can be trained on different devices without raw data transfer. FL has some

setbacks concerning security, scalability, trust, and a central aggregator's dependency. These issues are the reason for our project, “Secure Decentralized Aggregation for Privacy Protection in Edge-Based Federated Learning”, which aims to improve privacy, security, and efficiency of the system. The core issues with traditional federated learning (FL) systems stems from their reliance on a single, central server for coordinating the receiving and incorporating model updates from multiple clients. Such a design is inefficient due to it being a single point of failure, which exposes the system to vulnerabilities like cyber attacks, adversarial attacks, and data poisoning. In comparison, our method employs fully decentralized aggregation which eliminates the necessity for an aggregation server. Instead, we assign aggregation duties to different nodes, ensuring control over the model updates isn’t consolidated to one singular entity, thus, mitigating the problems accompanying centralization. This increases decentralization, system reliance, fault tolerance, and trust while simultaneously improving the system's resilience to failure and attack. In order to enhance data privacy in our project, we implement cryptographic technologies like Secure Multi-Party Computation (SMPC), Homomorphic Encryption (HE), and Differential Privacy (DP). These techniques guarantee that sensitive information is protected during secure aggregation of model updates. With SMPC, multiple participants can perform computations on their inputs and keep those inputs concealed. Similarly, encryption that supports homomorphic operations permits actions to be carried out on the encrypted information without revealing it. DP also ensures privacy is preserved by adding controlled noise to model updates, thus mitigating the potential for deduction of sensitive information. Combining these mechanisms ensures edge devices can participate in collaborative learning from distributed data in strict privacy. FL systems frequently experience inefficiencies and communication overhead in addition to privacy issues, particularly in edge environments with limited resources. Increased latency and bandwidth usage may result from frequent data transfers between devices and the central aggregator. By eliminating pointless data transfers and utilizing local model updates, our decentralized aggregation framework maximizes communication while guaranteeing effective use of network

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

resources. Our method is especially well-suited for applications in Internet of Things (IoT) networks, real-time decision-making systems, and smart environments where performance depends on minimizing latency. Beyond privacy and efficiency, trust and security are paramount in FL deployments, as malicious participants can attempt to manipulate global model updates through adversarial attacks. Traditional FL is vulnerable to model poisoning, Byzantine attacks, and sybil attacks, where compromised nodes introduce biased or incorrect updates to degrade model performance. Our project incorporates blockchain-based trust mechanisms and reputation-based aggregation to mitigate such risks. Blockchain technology ensures a transparent and tamper-proof record of model updates, preventing malicious activities. Additionally, reputation-based aggregation assigns higher influence to reliable nodes, reducing the impact of adversarial clients. This enhances the robustness and reliability of federated learning systems deployed in security-critical applications.

II.LITERATURE SURVEY

2.1Advances in Privacy-Preserving Federated Learning

Federated Learning (FL) has materialized as a distributed strategy for instructing machine learning models while obviating the need for the direct transmission of raw data. Nevertheless, apprehensions regarding privacy have instigated considerable scholarly inquiry into methodologies for secure aggregation. Numerous investigations have put forth the application of homomorphic encryption (HE), secure multi-party computation (SMPC), and differential privacy (DP) to guarantee the confidentiality of client-side updates throughout the model training lifecycle. These privacy-preserving strategies serve to lessen the potential for data breaches while upholding the efficiency of learning processes within FL systems operating at the network edge.

2.2 Decentralized Aggregation for Secure Model Training

Conventional methodologies in Federated Learning (FL) are predicated on a central server for the aggregation of models, thereby presenting a singular point of vulnerability and potential avenues for privacy compromise. To address these limitations, decentralized aggregation techniques, encompassing consensus mechanisms rooted in blockchain technology and peer-to-peer

(P2P) aggregation, have been developed to distribute the aggregation task across a multitude of nodes. Scholarly findings underscore the enhanced resilience to failures, heightened security, and improved scalability inherent in decentralized architectures within FL frameworks, especially in edge environments characterized by limited resources.

2.3 Challenges in Secure Federated Learning

Despite the progress achieved in privacy-preserving Federated Learning (FL), several inherent complexities persist. Research studies indicate that malicious clients can inject tampered model updates, which may compromise the accuracy of the final global model. To address such adversarial threats, various countermeasures have been explored, including Byzantine-robust aggregation protocols, anomaly detection systems, and frameworks for trust evaluation among participating entities. Additionally, computational overhead introduced by encryption methods remains a concern, requiring optimized cryptographic techniques to balance security and efficiency.

2.4 Efficient Aggregation Techniques for Edge-Based FL

Federated Learning (FL) systems operating at the network edge necessitate efficacious aggregation strategies to effectively manage the diverse computational and network capacities of participating devices. Scholarly inquiry has yielded techniques such as hierarchical aggregation, dynamic model compression, and client selection algorithms aimed at optimizing overall performance. These methodologies serve to diminish communication overhead, enhance the convergence rate of training, and refine the accuracy of the resultant model, thereby rendering FL a more viable option for real-world implementation.

2.5 Privacy and Security Enhancements for Federated Learning

To further fortify security within Federated Learning (FL) frameworks, researchers have explored hybrid encryption methodologies, secure enclaves, and zero-knowledge proofs (ZKP). Investigations indicate that the synergistic application of multiple privacy-preserving techniques can bolster resilience against inference attacks while ensuring adherence to data protection mandates. The integration of such sophisticated mechanisms into decentralized FL architectures represents an expanding frontier of research, yielding

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

promising outcomes in applications where the safeguarding of privacy is paramount..

III.EXISTING SYSTEM

Existing systems in edge-based Federated Learning (FL) primarily focus on enabling collaborative model training while ensuring data privacy by keeping raw data localized. These systems rely on centralized aggregation, where a central server collects and aggregates model updates from participating edge devices to update the global model.

IV.PROPOSED SYSTEM

The proposed system introduces a secure decentralized aggregation framework for edge-based Federated Learning (FL) to address the limitations of existing systems. By leveraging blockchain technology and an additive secret-sharing algorithm, the system ensures privacy preservation during the aggregation process without relying on a centralized server.

V.SYSTEM ARCHITECTURE

The architecture of the system is designed to ensure scalability, efficiency, and privacy protection while enabling secure decentralized aggregation in a federated learning environment. The architecture consists of the following layers:

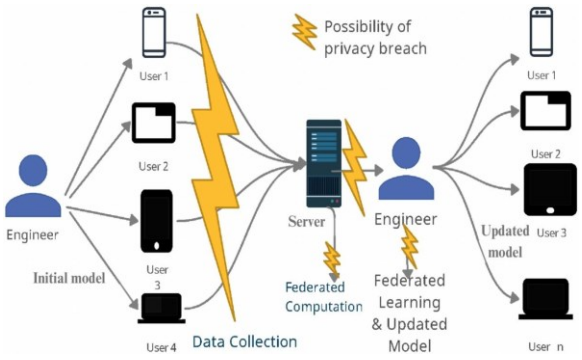

Figure 5.1 System Architecture

The client-side interface is built using HTML, CSS, and JavaScript, ensuring compatibility across multiple devices (desktops, tablets, and smartphones). It serves as the primary interaction point for users, where inputs are entered, and results are displayed

VI.OUTPUT SCREENSHOTS

Fig no: 6.1 Home Page

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

verifier users can securely access participate in the federated learning system

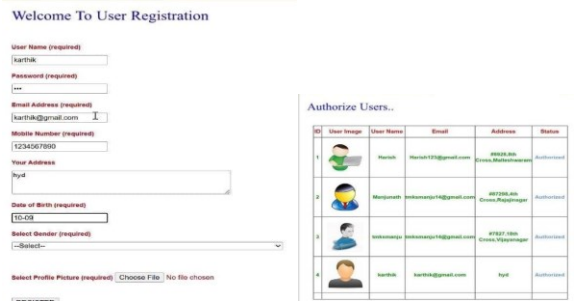

Fig no: 6.2 USER REGISTRATION AND AUTHORIZATION

Fig no: 6.3 Admin Page

Fig no: 6.4 Leakage Status

Fig no: 6.5 PRIVACY LEAKAGE ATTACKERS

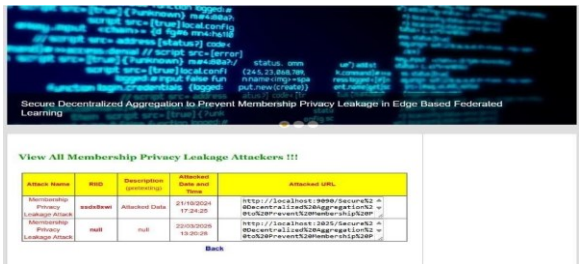

Fig no: 6.6 Leakage Attackers Status

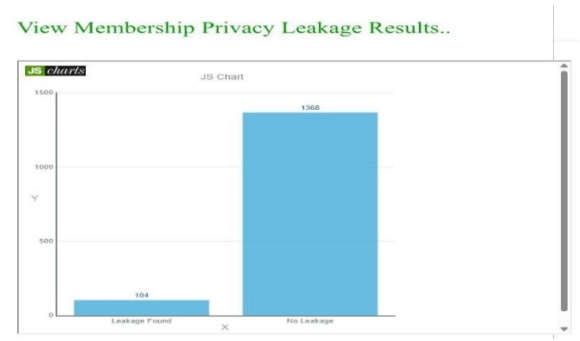

Fig no: 6.7Leakage Results

VII.CONCLUSION

This project presents a strong privacy-focused federated learning setup, using secure decentralized methods so user data stays on their devices via edge computing, minimizing risks and ensuring privacy. Encrypting model updates before sending them to the central server adds a crucial security layer, effectively reducing vulnerabilities to potential data leaks. Furthermore, strategically adding blockchain significantly strengthens the system's

security by proactively preventing membership inference and enhancing auditability without needing to reveal user identities. This tamper-proof approach strongly discourages unauthorized participation in the learning and ensures comprehensive accountability throughout. By employing secure aggregation protocols, the central server computes a global model without needing direct access to individual user data or their local model weights, thus upholding data confidentiality. Empirical validation through experiments and output analysis definitively confirms the system's effectiveness in maintaining high model accuracy while rigorously preserving the privacy of participating users.By using secure ways to combine information (secure aggregation protocols), the main computer can figure out an overall, unified model. It does this without ever needing to directly see the raw, individual user data. It also doesn't need to look at the specific learning that happened on each user's device, so confidentiality is maintained. In conclusion, this project offers a scalable and highly secure federated learning solution with significant realworld applicability in sensitive domains like healthcare and finance, where strong user privacy protection is paramount and cannot be compromised. This foundational project establishes a solid and promising groundwork for future research and the eventual real-time deployment of secure, privacy-aware AI systems across various distributed computing environments.

VIII.FUTURE SCOPE

1. Incorporate Differential Privacy

 Enhancement: Add noise to model updates to mask individual data contributions.

 Benefit: Enhances resistance to privacy leakage attacks.

 Implementation: Use differential privacy libraries like PySyft or TensorFlow Privacy to apply controlled noise to gradients.

2.Integrate Secure Multiparty Computation (SMPC)

 Enhancement: Enable several parties to calculate an output while keeping their individual inputs private.

 Benefit: Ensures total data confidentiality during aggregation.

 Implementation: Use SMPC frameworks like CrypTen or MP-SPDZ to perform encrypted computations.

3.Add Zero-Knowledge Proofs (ZKP)

 Enhancement: Implement a method to verify the accuracy of model updates without revealing the underlying data.

 Benefit: Builds trust in model contributions without compromising privacy.

 Implementation: Integrate ZKP protocols like zk-SNARKs using libraries such as libsnark.

4.Use Homomorphic Encryption

 Enhancement: Perform computations directly on encrypted data.

 Benefit: Prevents server-side data exposure entirely.

 Implementation: Use libraries like Microsoft SEAL or TenSEAL to implement encryption for training updates.

5. Dynamic Device Participation

 Enhancement: Implement dynamic joining and leaving of edge devices from the network.

 Benefit: Increases scalability and flexibility of the learning network.

 Implementation: Design a protocol with secure onboarding/offboarding steps and real-time syncing.

IX.REFERENCES

1) Ahmad et al. (2023) surveyed the applications of deep learning models in cloud, edge, fog, and IoT computing paradigms. Their work also covers recent advancements and future directions in this fields. Computer Sci Rev 49:100568

2) Arjovsky M, Chintala S, and Bottou L (2017) presented their work on Wasserstein generative adversarial networks in the Proceedings of the 34th International Conference on Machine Learning, volume 70, pages 214–223.PMLR, Sydney, NSW, Australia

3) Baracaldo N, Chen B, Ludwig H, Safavi JA (2017) Mitigating poisoning attacks on machine learning models: A data provenance-based approach.The findings were presented in the Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security, volume/pages 103–110. ACM, Dallas, Texas, USA

4) Bhagoji et al. (2019) presented their paper, 'Analyzing federated learning through an adversarial lens,' at the 36th International

Conference on Machine Learning, held in Long Beach, California, USA, and published by PMLR (pp. 634–643).

5) In their 2024 publication, Cao et al. detailed SRFL, a Secure & Robust Federated Learning framework. Designed specifically for IoT environments, SRFL tackles the inherent challenges and limitations of these settings..Expert Syst Appl 239:122410

6) Cao et al. (2024) presented SRFL, a Secure & Robust Federated Learning framework developed for IoT environments.. IEEE Trans Inf Forensics Secur 18:5749–5761

7) Fraboni et al. (2021) explored free-rider attacks on federated learning model aggregation (Proceedings of the 24th International Conference on Artificial Intelligence and Statistics, vol. 130, pp. 1846–1854, PMLR, Buenos Aires, Argentina).

8) In 2022, Guo JJ, Li HY, Huang FR, Liu ZQ, Peng YG, Li XH, Ma JF, Menon VG, and Igorevich KK presented ADFL, a framework designed to defend against poisoning attacks in horizontal federated learning. IEEE Trans Industr Inf 18(10):6526–6536

9) Li et al. (2023) published their study on model extraction attacks targeting split federated learning (arXiv preprint arXiv:2303.08581).

10) The authors, Chen et al. (2023), detailed APFed in IEEE Transactions on Information Forensics and Security (18:5749–5761). APFed is designed to mitigate poisoning attacks in heterogeneous federated learning while maintaining privacy.

11) Zhang et al. (2025) introduce FLPoison, a benchmark designed to standardize the evaluation of poisoning attacks and defenses in federated learning, offering a unified perspective on this critical security challenge.arXiv preprint arXiv:2502.03801.

12) Bai et al. (2024) present a comprehensive survey focusing on membership inference attacks and defenses within the context of federated learning, addressing a critical privacy concern in this domain.arXiv preprint arXiv:2412.06157.