(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :07/03/2026
(21) Application No.202641026949 A
(43) Publication Date : 20/03/2026

(54) Title of the invention : Federated Learning with Differential Privacy for Secure Multi-Device AI Applications

(51) International classification	:G06N 20/00, G06F 21/62, G06N 3/08, G06N 5/04, G06N 3/04
(31) Priority Document No	:NA
(32) Priority Date	:NA
(33) Name of priority country	:NA
(86) International Application No Filing Date	: :01/01/1900
(87) International Publication No	: NA
(61) Patent of Addition to Application Number Filing Date	:NA :NA
(62) Divisional to Application Number Filing Date	:NA :NA

(71)**Name of Applicant :**
1)Dr. A. Naga Malleswara Rao
Address of Applicant :Associate Professor, Department of Computer Science and Engineering, Sree Dattha Institute of Engineering and Science. Sheriguda Telangana India
2)Sreedevi Kadiyala
3)J. Supraja
4)V Vijayakumar Dasari
5)Puneet shetteppanapar
6)Dr.A.Manikandan
7)Dr.R.Poornima
8)G. Vidyu Latha
(72)**Name of Inventor :**
1)Dr. A. Naga Malleswara Rao
2)Sreedevi Kadiyala
3)J. Supraja
4)V Vijayakumar Dasari
5)Puneet shetteppanapar
6)Dr.A.Manikandan
7)Dr.R.Poornima
8)G. Vidyu Latha

(57) Abstract :
ABSTRACT [0013] The invention introduces a novel federated learning system enhanced with differential privacy techniques specifically designed for secure AI applications across multiple devices. This approach allows decentralized training of machine learning models where data remains on individual devices, preventing direct sharing and thus minimizing privacy risks. By integrating adaptive noise injection based on device-specific privacy budgets and real-time threat assessments, the system ensures robust protection against inference attacks while maintaining high model accuracy. Key innovations include a hierarchical aggregation protocol that combines local model updates with encrypted communications and a feedback loop for optimizing privacy parameters dynamically. This results in improved scalability for resource-constrained environments, such as mobile networks or IoT ecosystems, achieving up to 20% better privacy-utility trade-offs compared to traditional methods. The invention is applicable in fields like healthcare for patient data analysis, smart cities for traffic optimization, and personalized finance apps, all while upholding data sovereignty and compliance with privacy regulations.

No. of Pages : 9 No. of Claims : 7