पेटेंट कार्यालय
शासकीय जर्नल

OFFICIAL JOURNAL
OF
THE PATENT OFFICE

निर्गमन सं. 20/2026	शुक्रवार	दिनांक: 15/05/2026
ISSUE NO. 20/2026	FRIDAY	DATE: 15/05/2026

पेटेंट कार्यालय का एक प्रकाशन
PUBLICATION OF THE PATENT OFFICE

(12) PATENT APPLICATION PUBLICATION

(19) INDIA

(22) Date of filing of Application :01/04/2026

(21) Application No.202611041513 A

(43) Publication Date : 15/05/2026

(54) Title of the invention : A System and Method for Privacy-Preserving Decentralized Federated Learning on Resource-Constrained Edge Hardware

(51) International classification	:G06F 21/60, H04L 9/00, G06N 20/00, G06F 21/62, H04L 9/08
(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)Noida Institute of Engineering and Technology (NIET)
Address of Applicant :19, Institutional Area, Knowledge Park II, Greater Noida, Uttar Pradesh 201310 Uttar Pradesh India
(72)**Name of Inventor :**
1)Dr. Sangeeta Arora
2)Tushar

(57) Abstract :
The present invention relates to a hardware-accelerated system (100) and method for privacy-preserving decentralized federated learning of computer vision models deployed on resource-constrained edge processing units (101). The system addresses the critical technical problem of gradient-based data reconstruction attacks that compromise training data confidentiality even when raw data is retained locally. The invention integrates a CKKS-based homomorphic encryption engine (102) resident on a dedicated cryptographic co-processor (103), a threshold-adaptive gradient compression and Gaussian noise injection module (104) implemented in firmware on an embedded signal processing unit (105), and a peer-to-peer decentralized model aggregation controller (106) operating over a secure communication bus (107). By dynamically co-optimizing the gradient pruning ratio and noise variance as correlated hardware-controlled parameters within bounded accuracy-loss thresholds, the system achieves reconstruction resistance against Deep Leakage from Gradients attacks while constraining model accuracy degradation to below 4 percent, enabling deployable privacy-preserving collaborative training across distributed industrial edge devices.

No. of Pages : 22 No. of Claims : 10