Indian Patent Advanced Search System (http://ipindia.nic.in/index.htm)

INTELLECTUAL PROPERTY INDIA
PATENTS | DESIGNS | TRADE MARKS
GEOGRAPHICAL INDICATIONS
(http://ipindia.nic

Patent Search

Invention Title	A SYSTEM AND METHOD FOR PRIVACY-PRESERVING DATA SCIENCE USING FEDERATED LEARNING
Publication Number	35/2025
Publication Date	29/08/2025
Publication Type	INA
Application Number	202541079141
Application Filing Date	20/08/2025
Priority Number	
Priority Country	
Priority Date	
Field Of Invention	COMPUTER SCIENCE
Classification (IPC)	G06F0021620000, G06N0020000000, H04L0009000000, G06F0021600000, H04L0009400000

Inventor

Name	Address	Country
Ms. Sunkavilli Vijaya Nirmala	Assistant Professor, Department of CSE- AIML, Aditya University, Surampalem, Kakinada, Andhra Pradesh, India. Pin Code:533437	India
Mr. Vorem Kishore	Assistant Professor, Department of CSE-AIML & IOT, VNR Vignana Jyothi Institute of Engineering & Technology, Pragathinagar, Nizampet(S.O), Hyderabad, Telangana, India. Pin Code: 500090	India
Mr. M. Hari Krishna Marrapu	Assistant Professor, Department of Information Technology, GMR Institute of Technology, Rajam, Vizianagaram District, Andhra Pradesh, India. Pin Code:532127	India
Dr. Pradeep Venuthurumilli	Associate Professor, Department of CSE- Data Science, Malla Reddy Engineering College for Women, Maisammaguda, Secunderabad, Telangana, India. Pin Code:500100	India
Dr. Anandbabu Gopatoti	Professor & Ho D, Department of Electronics and Communication Engineering, Welfare Institute of Science, Technology & Management, Pinagadi, Visakhapatnam, Andhra Pradesh, India, Pin Code: 530047	India
Ms. V. Dhanakodi	Assistant Professor, Department of CSE, Mahendra College of Engineering, Minnampalli, Salem, Tamil Nadu, India. Pin Code:636106	India
Mrs. M. Gayathri	Assistant Professor, Department of CSE, Mahendra College of Engineering, Minnampalli, Salem, Tamil Nadu, India. Pin Code:636106	India
Dr. M. Lakshmiprasad	Professor and Head, Department of CSE, Institute of Aeronautical Engineering, Dundigal, Hyderabad, Telangana, India. Pin Code: 500043	India
Prof. Sharon Rajendra Manmothe	Assistant Professor, School of Computer Studies, Shri Balaji University, Pune, Maharashtra, India. Pin Code:411033	India
Mr. Ravishankar C. Bhaganagare	Assistant Professor, Department of CSE (AI&ML), Vishwakarma Institute of Technology, Pune, Maharashtra, India. Pin Code:411037	India

Applicant

Name	Address	Country
Ms. Sunkavilli Vijaya Nirmala	Assistant Professor, Department of CSE- AIML, Aditya University, Surampalem, Kakinada, Andhra Pradesh, India. Pin Code:533437	India
Mr. Vorem Kishore	Assistant Professor, Department of CSE-AIML & IOT, VNR Vignana Jyothi Institute of Engineering & Technology, Pragathinagar, Nizampet(S.O), Hyderabad, Telangana, India. Pin Code: 500090	India
Mr. M. Hari Krishna Marrapu	Assistant Professor, Department of Information Technology, GMR Institute of Technology, Rajam, Vizianagaram District, Andhra Pradesh, India. Pin Code:532127	India
Dr. Pradeep Venuthurumilli	Associate Professor, Department of CSE- Data Science, Malla Reddy Engineering College for Women, Maisammaguda, Secunderabad, Telangana, India. Pin Code:500100	India
Dr. Anandbabu Gopatoti	Professor & Ho D, Department of Electronics and Communication Engineering, Welfare Institute of Science, Technology & Management, Pinagadi, Visakhapatnam, Andhra Pradesh, India, Pin Code: 530047	India
Ms. V. Dhanakodi	Assistant Professor, Department of CSE, Mahendra College of Engineering, Minnampalli, Salem, Tamil Nadu, India. Pin Code:636106	India
Mrs. M. Gayathri	Assistant Professor, Department of CSE, Mahendra College of Engineering, Minnampalli, Salem, Tamil Nadu, India. Pin Code:636106	India
Dr. M. Lakshmiprasad	Professor and Head, Department of CSE, Institute of Aeronautical Engineering, Dundigal, Hyderabad, Telangana, India. Pin Code: 500043	India
Prof. Sharon Rajendra Manmothe	Assistant Professor, School of Computer Studies, Shri Balaji University, Pune, Maharashtra, India. Pin Code:411033	India
Mr. Ravishankar C. Bhaganagare	Assistant Professor, Department of CSE (AI&ML), Vishwakarma Institute of Technology, Pune, Maharashtra, India. Pin Code:411037	India

Abstract:

045] The present invention discloses a federated learning framework for privacy-preserving data science applications that enables collaborative machine learning acr distributed datasets without requiring centralization of sensitive information. The framework comprises a plurality of client devices configured to perform local mode differential privacy module for injecting calibrated noise into updates, and an encryption module for securing model parameters during transmission. A secure aggre combines encrypted updates using adaptive weighting algorithms to account for heterogeneous and non-IID client data, while preventing access to individual contrib blockchain-based audit layer records update transactions in an immutable ledger, ensuring transparency, accountability, and tamper-proof traceability of client partic system further includes communication optimization protocols for compressing model updates and dynamic scheduling of client participation, making it suitable for environments. An anomaly detection module safeguards against malicious or poisoned updates, thereby maintaining model integrity. By integrating privacy, security, and accountability into a unified design, the invention advances federated learning and finds applications in healthcare, finance, IoT, government analytics, and other requiring secure and privacy-preserving data science. Accompanied Drawing [FIGS. 1-2]

Complete Specification

Description:[001] The present invention relates generally to the field of data science and artificial intelligence, and more particularly, to a federated learning framew enables collaborative machine learning across distributed datasets while ensuring privacy-preserving data analytics.

[002] Specifically, the invention provides a system and method for secure, efficient, and scalable federated learning by integrating differential privacy, secure aggreg encryption, and blockchain-based audit mechanisms to safeguard sensitive data in domains such as healthcare, finance, Internet of Things (IoT), and other regulate industries.

BACKGROUND OF THE INVENTION

[003] In recent years, machine learning and artificial intelligence (AI) have become integral to modern data-driven applications across sectors such as healthcare, ba commerce, and IoT-enabled smart environments. These applications rely heavily on large-scale data collection and centralized training of machine learning models. However, centralizing sensitive data presents significant challenges regarding privacy, regulatory compliance, and data security.

[004] Traditional centralized machine learning approaches require raw data to be transmitted and stored in a central server or cloud infrastructure. This practice ex sensitive information to risks such as unauthorized access, data breaches, and malicious misuse. Moreover, compliance with privacy regulations like the General Da Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) makes centralized data aggregation impractical in many cases.

[005] To address these concerns, federated learning has been proposed as a decentralized machine learning paradigm. In this approach, models are trained locally devices or institutional servers, and only model parameters or gradients are shared with a coordinating server. This eliminates the need to transfer raw data, therek reducing privacy risks. However, federated learning in its current form is still subject to limitations that hinder widespread adoption.

View Application Status

Department of Industrial Policy and Promotion
Government of India

Terms & conditions (https://ipindia.gov.in/Home/Termsconditions) Privacy Policy (https://ipindia.gov.in/Home/Privacypolicy) Copyright (https://ipindia.gov.in/Home/copyright) Hyperlinking Policy (https://ipindia.gov.in/Home/hyperlinkingpolicy) Accessibility (https://ipindia.gov.in/Home/accessibility) Contact Us (https://ipindia.gov.in/Home/contactus) Help (https://ipindia.gov.in/Home/help)

Content Owned, updated and maintained by Intellectual Property India, All Rights Reserved.