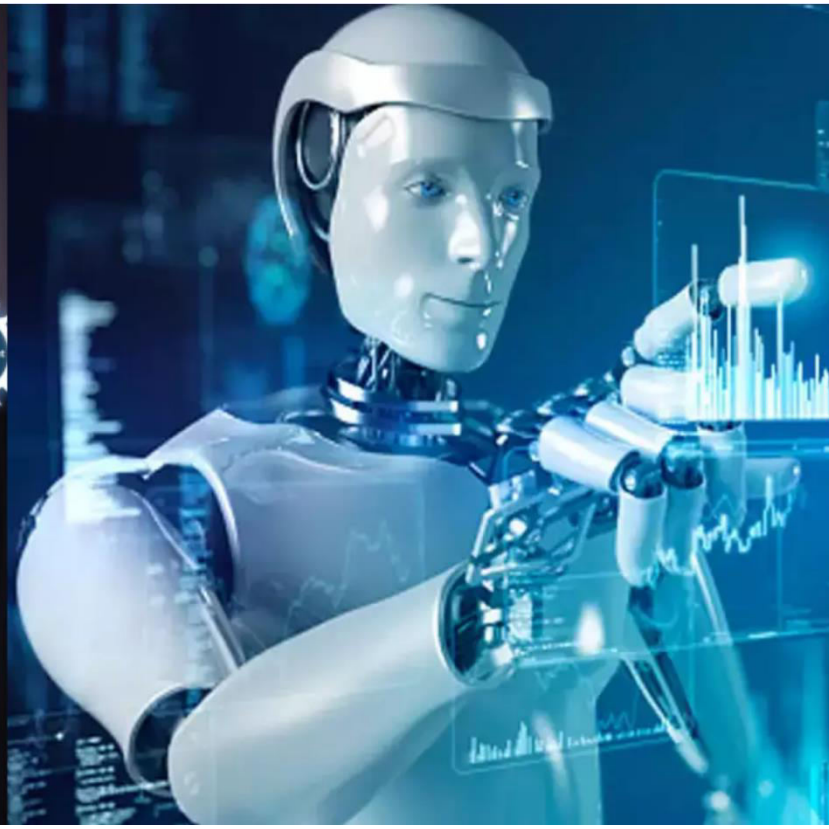
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Issue 3, March 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503328|

Privacy Preserving AI Platform Using Federated Learning

A. Loganayaki[1], Arulkumar J[2], Dhasnamoorthy D[3], Gowtham V[4], Gokulraj K[5]

Assistant Professor, Department of Information Technology, The Kavery Engineering College (Autonomous), Mecheri, Salem, Tamil Nadu, India[1]

UG Students, Department of Information Technology, The Kavery Engineering College (Autonomous), Mecheri, Salem, Tamil Nadu, India. [2,3,4,5]

ABSTRACT: Privacy concerns remain a major challenge in the adoption of artificial intelligence systems that rely on large-scale data collection and centralized learning. This project proposes a Privacy-Preserving AI Platform using Federated Learning, enabling multiple distributed clients to collaboratively train a shared AI model while keeping sensitive data on local devices. Unlike traditional centralized approaches, the system ensures data confidentiality by exchanging only model updates, thereby reducing privacy risks and enhancing user trust. Contract review is a critical legal task that involves several processes such as compliance validation, clause classification, and anomaly detection. Traditional, centralized models for the analysis of contracts raise significant data privacy and compliance challenges due to the highly sensitive nature of legal documents. This paper proposes a contract review-oriented federated learning framework, where model training can be performed in a completely decentralized way with data confidentiality. It leverages privacy preserving methods such as Differential Privacy ("DP") and Secure Multi-Party Computation ("SMPC") that provide protection for sensitive information during collaborative learning. The proposed framework reaches a clause classification accuracy of 94.2% while securing privacy requirements. Performance analysis of the training efficiency revealed that the federated model needed 13.1 hours instead of 10.4 hours for a centralized model while still protecting the security of the system. This research offers a scalable and secure approach toward contract review and offers a path forward for privacy-conscious AI-driven legal solutions.

I. INTRODUCTION

The rise of cloud-based database management systems has enabled organizations to process vast amounts of data efficiently. However, concerns over data privacy, security, and regulatory compliance necessitate innovative

solutions for AI-driven data analysis. Federated learning has emerged as a promising approach that enables machine learning models to be trained across decentralized data sources without exposing sensitive information. This paper explores the integration of federated learning with cloud-based database management to ensure privacypreserving AI operations. It examines key challenges such as data heterogeneity, communication overhead, security risks, and performance trade-offs. Furthermore, it discusses how federated learning enhances privacy while maintaining model accuracy and scalability in cloud environments. Experimental results demonstrate that federated learning can achieve comparable model performance to centralized learning while preserving data confidentiality. This study provides a comprehensive analysis of federated learning's potential in cloud database management, addressing practical implementations, security measures, and future research directions.

Cloud-based database management systems have revolutionized data storage, retrieval, and processing. These systems allow organizations to leverage distributed infrastructure for efficient data management. However, as AI-driven analytics become more prevalent, the need to ensure privacy and security of sensitive data has become a major challenge. Traditional machine learning methods often require data to be centralized, which can pose risks related to unauthorized access, data breaches, and regulatory non-compliance.

1.1. OVERVIEW

Federated learning offers an alternative by enabling collaborative model training across multiple devices or institutions while keeping raw data localized. Instead of transferring sensitive data to a central server, federated learning sends

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503328|

model updates, reducing privacy risks. This decentralized learning paradigm has significant implications for cloud-based database management, where data is often distributed across multiple locations and governed by strict compliance requirements. This paper explores how federated learning can enhance privacy-preserving AI in cloud database management. It examines the advantages, limitations, and implementation challenges of federated learning in this context. Additionally, it evaluates security risks and proposes strategies to mitigate vulnerabilities. The study aims to provide insights into the feasibility and effectiveness of federated learning for organizations seeking to leverage AI without compromising data privacy The study investigates the application of federated learning in cloud-based database management by designing a federated learning framework tailored for privacy-preserving AI. The framework consists of a central server that coordinates learning tasks while maintaining data locality across multiple cloud database instances. A simulated cloud environment is used to evaluate the performance of federated learning in a distributed setting. The experimental setup includes multiple client nodes representing distinct cloud database clusters. Each node trains a local model on its dataset and periodically shares model updates with the central aggregator. The central server performs federated averaging to update the global model without accessing raw data. The datasets used in the study include structured and unstructured data commonly found in cloudbased databases, such as customer transactions, financial records, and sensor logs. The model architecture is based on deep learning techniques, including convolutional neural networks (CNNs) and recurrent neural networks (RNNs), depending on the nature of the data. To assess the effectiveness of federated learning, the study evaluates performance metrics such as model accuracy, training convergence, and communication efficiency. Additionally, security mechanisms such as homomorphic encryption and differential privacy are integrated into the framework to enhance privacy protection. The impact of data heterogeneity on model performance is analyzed by introducing variations in data distributions across client nodes.

II. LITERATURE REVIEW

1. A Review on Federated Learning Architectures for Privacy-Preserving AI: Lightweight and Secure Cloud–Edge–End Collaboration

Federated learning (FL) has emerged as a promising paradigm for enabling collaborative training of machine learning models while preserving data privacy. However, the massive heterogeneity of data and devices, communication constraints, and security threats pose significant challenges to its practical implementation. This paper provides a system review of the state-of-the-art techniques and future research directions in FL, with a focus on addressing these challenges in resource-constrained environments by a cloud–edge–end collaboration FL architecture. We first introduce the foundations of cloud–edge–end collaboration and FL. We then discuss the key technical challenges. Next, we delve into the pillars of trustworthy AI in the federated context, covering robustness, fairness, and explainability. We propose a dimension reconstruction of trusted AI and analyze the foundations of each trustworthiness pillar. Furthermore, we present a lightweight FL framework for resource-constrained edge–end devices, analyzing the core contradictions and proposing optimization paradigms. Finally, we highlight advanced topics and future research directions to provide valuable insights into the field.

2. Federated Learning Optimization for Privacy-Preserving AI in Cloud Environments

The growing dependence on cloud-based AI applications has raised concerns regarding data privacy, security, and computing efficiency. Traditional AI models are susceptible to privacy and security issues due to their reliance on centralized data aggregation. Federated Learning (FL) has emerged as a promising solution that enables decentralized model training without sharing raw data. However, FL faces critical challenges, including communication overhead, slow convergence rates, and privacy leakage risks. This study introduces an optimized FL framework that integrates gradient compression techniques to reduce communication overhead and employs differential privacy mechanisms to enhance data security. We evaluate our approach using the NSL-KDD dataset, which consists of 41 network traffic features. Our experimental results show that the proposed method achieves 97.4% accuracy, surpassing baseline FL techniques such as FedAvg (92.5%), FedAvg with Gradient Compression (93.8%), and FedAvg with Differential Privacy (91.2%). Additionally, our model achieves faster convergence with only 120 communication rounds and significantly reduces privacy leakage to 2.1%. This work proposes a privacy-preserving and scalable FL framework that improves security and efficiency in cloud-based AI environments, providing a workable solution for practical cybersecurity and other applications.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503328|

3. FEDERATED LEARNING AND PRIVACY-PRESERVING AI

The rapid digitization of enterprises and the proliferation of data across geographies have elevated privacy and data sovereignty to critical concerns in artificial intelligence (AI) development. Federated Learning (FL) has emerged as a powerful paradigm for training machine learning models across decentralized data silos without compromising user privacy. This article presents a comprehensive technical study of federated learning and its integration with privacy-preserving technologies such as differential privacy, secure multiparty computation, and homomorphic encryption. Emphasis is placed on the unique challenges and opportunities of applying FL in SaaS (Software-as-a-Service) platforms like ServiceNow, where multi-tenancy and data regulation create constraints that traditional centralized models cannot address. We examine baseline FL architecture such as FedAvg, FedProx, and personalized FL strategies and assess privacy-involving techniques with practical source considerations. The article provides a case of federated incident prediction across isolated tenants in a SaaS environment, showing a substantial performance gain without compromising the data privacy regulation. Selected results indicate the practical applicability of FL in cross-organization learning, especially in high-consequence areas of IT service management and healthcare. This work offers architectural blueprints, experimental benchmarks, and technical guidance for adopting federated models within enterprise SaaS systems. It further discusses societal and ethical considerations surrounding trust, transparency, and fairness in federated AI systems. The article contributes original insights supporting claims of significant technical innovation and impact, aligning strongly with EB1A/B criteria for exceptional AI and software engineering.

III. IMPLEMENTATION

EXISTING SYSTEM

- User data from all devices is collected and stored in a central server.
- Centralized data aggregation creates a single point of failure.
- Large-scale data storage increases the risk of data breaches.
- Privacy of users is compromised due to centralized model training.

3.1. DISADVANTAGES OF EXISTING SYSTEM

- Centralized data storage increases the risk of data breaches and privacy loss.
- Sharing sensitive data with central servers reduces user trust.
- Centralized systems have a single point of failure and security risks.
- Scalability and regulatory compliance are difficult in centralized AI systems.

3.2. PROPOSED SYSTEM

- User data is trained locally on devices without sharing raw data.
- Only encrypted model parameters are sent to the central server.
- The server aggregates updates using federated learning algorithms.
- A global model is improved while preserving user data privacy.

3.2.1. ADVANTAGES

- ✓ User data stays on local devices, ensuring strong data privacy.
- ✓ Federated learning enables decentralized and secure model training.
- ✓ Transparent and secure mechanisms improve user trust and safety.
- ✓ Distributed learning improves scalability while maintaining accuracy.

WORKING

1. Privacy Confidence Score Module

Description:

The Privacy Confidence Score module evaluates the level of data privacy and security maintained by the system when handling user information.

Explanation:

This module analyzes various privacy-related factors such as data encryption, secure authentication methods, and access control policies. It calculates a privacy confidence score that indicates how well the system protects sensitive

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503328|

information. The score is generated by evaluating security practices and compliance with privacy standards. This helps system administrators monitor privacy protection levels and ensure that user d.ata remains secure

2. Federated Trust-Based Client Ranking Module
Description:
The Federated Trust-Based Client Ranking module ranks system clients based on their trustworthiness in a federated learning environment.

Explanation:
In federated systems, multiple clients contribute data to train a shared model. This module evaluates each client's reliability by analyzing the quality and consistency of the data they provide. Clients with reliable contributions receive higher trust scores, while suspicious or inconsistent contributors receive lower rankings. This process ensures that the overall learning system remains accurate and resistant to malicious or low-quality data contributions.

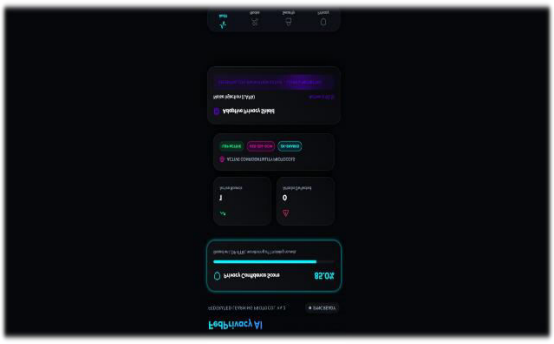
3. Adaptive Privacy Shield Module
Description:
The Adaptive Privacy Shield module dynamically protects sensitive data by applying privacy mechanisms based on system conditions.

Explanation:
This module monitors system activity and adjusts privacy protection techniques accordingly. It may apply encryption, anonymization, or data masking depending on the level of risk detected. For example, if sensitive user information is being accessed frequently, the system automatically increases privacy safeguards. This adaptive mechanism ensures continuous protection against unauthorized access and privacy breaches.

4. Silent Attack Detection Engine Module
Description:
The Silent Attack Detection Engine identifies hidden or stealthy cyber attacks that attempt to compromise system security without triggering obvious alerts.

Explanation:
This module continuously monitors system behavior, network traffic, and data access patterns to detect suspicious activities. It uses anomaly detection techniques to identify unusual patterns that may indicate silent attacks such as data manipulation or unauthorized system access. When abnormal behavior is detected, the system alerts administrators and records the event for further analysis. This proactive approach helps maintain system integrity and security.

IV. SAMPLE OUTPUT



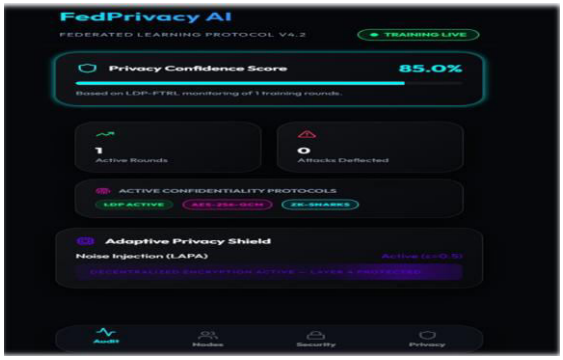
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

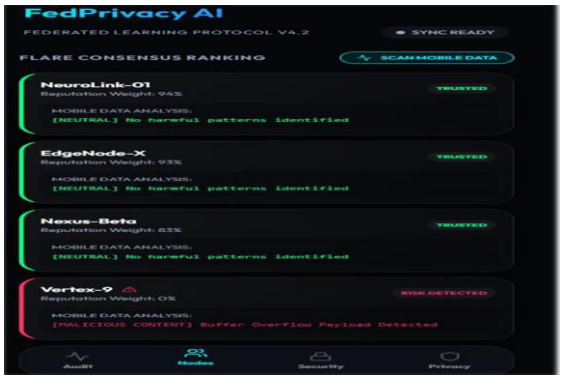
Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503328|





V. CONCLUSION

The Privacy-Aware Intelligent Security System enhances data protection and system reliability by integrating advanced privacy and security mechanisms. Modules such as the Privacy Confidence Score, Federated Trust-Based Client Ranking, Adaptive Privacy Shield, and Silent Attack Detection Engine work together to maintain a secure environment for data processing and communication.

These modules ensure that sensitive data remains protected, trustworthy clients contribute to the system, and potential cyber threats are detected early. By combining privacy evaluation, adaptive protection strategies, and intelligent monitoring techniques, the system significantly improves security, transparency, and trust in modern digital platforms

REFERENCES

1. Ian Sommerville, *Software Engineering*, Pearson Education.
2. Roger S. Pressman, *Software Engineering: A Practitioner's Approach*, McGraw-Hill.
3. Stuart Russell & Peter Norvig, *Artificial Intelligence: A Modern Approach*, Pearson.
4. Daniel Jurafsky & James H. Martin, *Speech and Language Processing*, Pearson.
5. Christopher Manning, *Introduction to Information Retrieval*, Cambridge University Press.
6. Python Software Foundation Documentation – https://docs.python.org
7. Scikit-Learn Machine Learning Library – https://scikit-learn.org
8. IEEE Xplore Digital Library – Federated Learning and Security Research Papers.
9. ACM Digital Library – Privacy-Preserving Machine Learning Studies.
10. Research studies on cybersecurity, federated learning security, and privacy-preserving AI systems.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details