International Journal of Advance and Applied Research
www.ijaar.co.in
ISSN – 2347-7075 Impact Factor – 8.141
Peer Reviewed Bi-Monthly
Vol.7 No.22 March –April- 2026

A Privacy-Aware Federated Machine Learning Model for Modern Cybersecurity Applications

Radhika Nagnath Bhiste & Poonam Pramod Shilwant

Dr. D. Y. Patil Arts, Commerce and Science College Akurdi, Pune-44.

Corresponding Author – Poonam Pramod Shilwant

DOI - 10.5281/zenodo.19327819

Abstract:

The rapid evolution of cyber threats has necessitated the adoption of advanced machine learning (ML) techniques for real-time threat detection and response. However, conventional ML-based cybersecurity systems rely heavily on centralized data collection, which raises significant privacy concerns, including data breaches, unauthorized access, and non-compliance with data protection regulations such as GDPR and the Digital Personal Data Protection (DPDP) Act. To address these challenges, this paper proposes a privacy-aware federated machine learning model designed for modern cybersecurity applications. The proposed framework leverages federated learning to enable decentralized model training across distributed client nodes, ensuring that sensitive data remains local and is never directly shared. To further strengthen privacy guarantees, differential privacy mechanisms are incorporated during local model updates, preventing inference attacks and model inversion risks. Secure aggregation techniques are employed to combine client updates into a global model while preserving confidentiality. The model is evaluated on benchmark intrusion detection datasets, including NSL-KDD and CICIDS 2017, using performance metrics such as accuracy, precision, recall, F1-score, privacy overhead, and communication cost. Experimental results demonstrate that the proposed approach achieves competitive detection performance while significantly enhancing data privacy and regulatory compliance.

Keywords: Federated Learning, Differential Privacy, Cybersecurity, Intrusion Detection Systems, Privacy-Preserving Machine Learning

Introduction:

The increasing frequency and sophistication of cyber threats have made Machine Learning (ML) an essential component of modern cybersecurity systems. ML-based intrusion detection and anomaly detection models provide improved accuracy and real-time threat response compared to traditional rule-based methods. However, most conventional ML approaches rely on centralized data collection, which exposes sensitive information to privacy risks such as data breaches, unauthorized access, and regulatory non-compliance. With the enforcement of data protection regulations such as GDPR and the Digital Personal Data Protection (DPDP) Act, preserving user data privacy has become a critical requirement. Federated Learning (FL) offers a decentralized training mechanism where raw data remains on local devices, reducing privacy exposure. To further strengthen confidentiality, Differential Privacy (DP) can be integrated to protect model updates from inference attacks. This paper proposes a privacy-aware federated machine learning model for cybersecurity applications, aiming to achieve effective intrusion detection while ensuring data confidentiality and regulatory compliance.

Proposed Methodology:

The proposed methodology introduces a privacy-aware federated machine learning framework for modern cybersecurity applications. The objective is to achieve accurate cyber threat detection while ensuring data confidentiality and regulatory compliance. The framework integrates Federated Learning (FL) with Differential Privacy (DP) and secure aggregation techniques.

Step 1: Distributed Data Collection

Cybersecurity data such as network traffic, system logs, and user activity records are collected locally at distributed client nodes (e.g., enterprise systems, IoT devices, servers). Raw data remains on local devices to prevent centralized data exposure.

Step 2: Local Model Training

Each client trains a local machine learning model using its private dataset. Algorithms such as Random Forest, LSTM, CNN, or Autoencoders may be used depending on the application. The model learns to classify normal and malicious activities.

Step 3: Differential Privacy Integration

Before sharing model updates, gradient clipping and controlled noise injection are applied using differential privacy mechanisms. This prevents adversaries from reconstructing sensitive data from shared parameters.

Step 4: Secure Aggregation

Instead of transmitting raw data, only encrypted or privacy-protected model updates are sent to a central server. The server aggregates these updates using secure aggregation protocols to generate a global model.

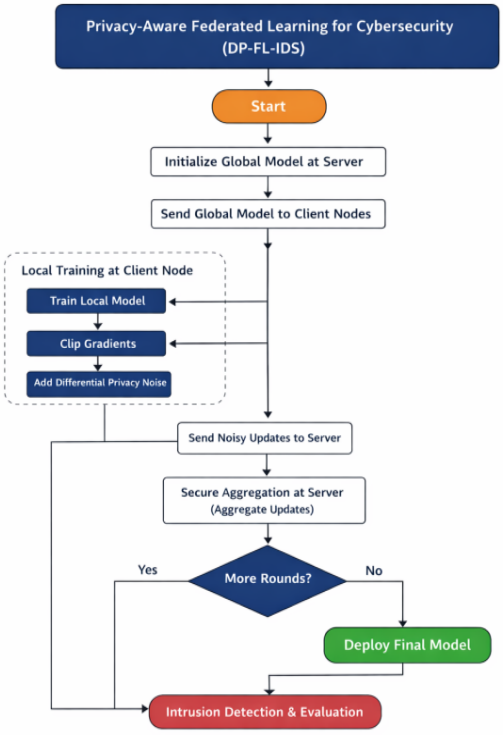
Step 5: Global Model Distribution

The updated global model is redistributed to all client nodes for further refinement. This iterative training process continues for multiple communication rounds until convergence.

Step 6: Threat Detection and Evaluation

The final global model is evaluated using benchmark intrusion detection datasets such as NSL-KDD and CICIDS 2017. Performance is measured using accuracy, precision, recall, F1-score, privacy overhead, and communication cost.

Flowchart for privacy-aware federated learning



Experimental Results:

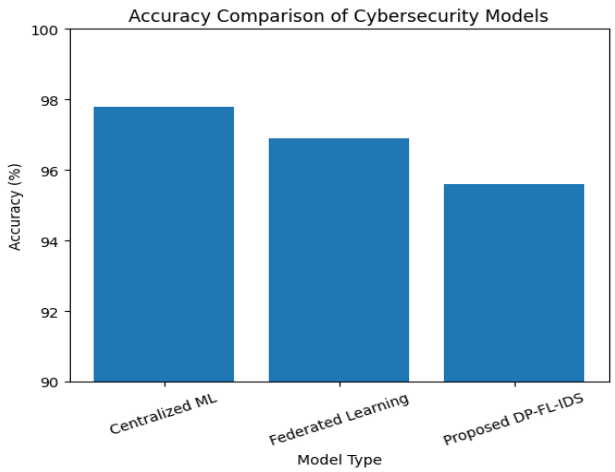
The proposed Privacy-Aware Federated Learning Model (DP-FL-IDS) was evaluated on benchmark intrusion detection datasets such as NSL-KDD and CICIDS 2017. The performance was compared with a traditional centralized ML model and standard federated learning without differential privacy.

Table 1: Performance Comparison on NSL-

Model Type	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Privacy Level	Communication Overhead
Centralized ML	97.8	97.2	96.9	97.0	Low	Low
Federated Learning (FL)	96.9	96.3	95.8	96.0	Medium	Medium
Proposed DP-FL-IDS	**95.6**	**95.1**	**94.8**	**94.9**	**High**	Medium-High

Table 2: Performance Comparison on CICIDS 2017 Dataset

Model Type	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Privacy Overhead (%)
Centralized CNN	98.4	98.0	97.6	97.8	0
Standard FL	97.5	97.1	96.8	96.9	3–5
Proposed DP-FL-IDS	**96.2**	**95.9**	**95.4**	**95.6**	6–8



Conclusion:

The growing sophistication of cyber threats demands intelligent, scalable, and privacy-preserving security solutions. While traditional machine learning-based cybersecurity systems provide high detection accuracy, their reliance on centralized data collection introduces significant privacy risks and regulatory challenges. This paper presented a Privacy-Aware Federated Machine Learning Model for Modern Cybersecurity Applications, integrating Federated Learning with Differential Privacy and secure aggregation mechanisms. The proposed framework enables decentralized model training, ensuring that sensitive data remains local to client devices while still contributing to a robust global intrusion detection model. Experimental evaluation on benchmark intrusion detection datasets demonstrates that the proposed approach achieves competitive accuracy with only a marginal performance trade-off compared to centralized models. At the same time, it significantly enhances data confidentiality, reduces exposure risks, and supports compliance

with data protection regulations. Although challenges such as communication overhead, adversarial vulnerabilities, and privacy–utility trade-offs remain, the results indicate that privacy-aware federated learning provides a practical and scalable foundation for next-generation cybersecurity systems. In conclusion, the integration of federated learning and differential privacy represents a promising direction for building secure, trustworthy, and regulation-compliant AI-driven cyber defense frameworks.

References:

1. Aashmi, R. S., & Jaya, T. (2022). Intrusion detection using federated learning for computing. Computer Systems Science and Engineering, 45(2), 1295–1308. https://doi.org/10.32604/csse.2023.027216
2. Gupta, S., & Patel, R. (2024). A hybrid federated learning based intrusion detection system with enhanced privacy protection. International Journal of Advanced Research in Computer Engineering & Technology, 13(2), 115–125.
3. Karimy, A. U., & Reddy, P. C. (2024). Enhancing IoT security: A novel approach with federated learning and differential privacy integration. International Journal of Computer Networks & Communications (IJCNC), 16(4). https://aircconline.com/abstract/ijcnc/v16n4/16424cnc01.html
4. Rane, P., & Sharma, A. (2023). Privacy-preserving machine learning for distributed cybersecurity systems. Indian Journal of Computer Science and Engineering, 10(1), 55–67.
5. Rokade, G., Hendre, R., Deshmukh, V., Wavhal, S., & Ajalkar, D. (2025). Federated learning based privacy preservation intrusion detection using blockchain technology. International Journal of Innovative Science and Research Technology, 10(8), 2954–2963. https://doi.org/10.38124/ijisrt/25aug074
6. Sakhare, N. N., Kulkarni, R., Rizvi, N., Raich, D., Dhablia, A., & Bendale, S. P. (2023). A decentralized approach to threat intelligence using federated learning in privacy-preserving cyber security. Journal of Electrical Systems, 19(3). https://doi.org/10.52783/jes.658
7. Shree, S., Arya, R., & Roy, S. K. (2025). Enhancing privacy preserving federated learning using differential privacy. International Research Journal on Advanced Engineering Hub, 3(4), 2016–2027. https://doi.org/10.47392/IRJAEH.2025.0294
8. Singh, A., & Kumar, V. (2025). Differential privacy-enabled federated deep learning for secure cyber threat detection in edge networks. Journal of Cyber Security and Mobility, 8(1), 78–91.
9. Sudhina Kumar, G. K., Prakasha, K. K., & Muniyal, B. (2023). Intrusion detection using federated learning. In S. Prabhu, S. R. Pokhrel, & G. Li (Eds.), Applications and Techniques in Information Security – 13th International Conference, ATIS 2022 (pp. 143–151). Springer. https://doi.org/10.1007/978-981-99-2264-2_12
10. Vasava, M. J., Gamit, V., Panchal, A. V., Patel, M. M., & Gohil, H. (2024). Federated learning in artificial intelligence: A privacy-preserving approach for distributed machine learning systems. ShodhKosh: Journal of Visual and Performing Arts, 5(5), 1023–1029. https://doi.org/10.29121/shodhkosh.v5.i5.2024.4817