Babylonian Journal of Networking
Vol.2026, **pp**. 32–37
DOI: https://doi.org/10.58496/BJN/2026/004; ISSN: 3006-5372
https://mesopotamian.press/journals/index.php/BJN

Research Article

A Federated Deep Learning Framework for Privacy-Preserving Digital Identity Anomaly Detection in Distributed Networks

Ing. Roman Danel [1,*]

[1] *Department of Mechanical Engineering, Faculty of Technology, Institute of Technology and Business in České Budějovice, Czech Republic*.

ARTICLE INFO

Article History

Received 04 Jun 2026
Revised 16 Jul 2026
Accepted 03 Aug 2026
Published 31 Aug 2026

Keywords
Federated Learning,
Deep Learning,
Digital Identity,
Anomaly Detection,
Privacy Preservation.

ABSTRACT

The increasing use of distributed digital services has created significant challenges in detecting identity anomalies while protecting sensitive user information. This study develops a federated deep learning framework for privacy-preserving digital identity anomaly detection in distributed networks. The research focuses on decentralized learning, where identity-related data remain within participating client environments, and only model parameters are exchanged for collaborative training. The methodology includes data preprocessing, local deep learning, federated parameter aggregation, privacy protection, anomaly classification, and performance evaluation. The experimental results demonstrate that the proposed approach achieves 98.76% accuracy, 98.42% precision, 98.61% recall, and 98.51% F1-score. The federated training analysis further shows progressive improvement across communication rounds, reaching 97.68% validation accuracy and a 98.21% detection rate. These findings indicate that federated deep learning can effectively support distributed identity anomaly detection while reducing direct exposure of sensitive identity data. The framework provides a foundation for secure and scalable identity analytics in networked environments.

1. INTRODUCTION

The concept of digital identity has been recognized as a critical element of networking services, online transactions, distributed systems, and interconnected digital spaces. The growing reliance on biometrics, behavioral information, transaction history, and context-driven identity elements necessitates the development of robust approaches to detect any unusual identity behavior. State-of-the-art approaches for identity verification have shown that heterogeneous identity information is useful in generating enhanced identity representation in order to differentiate between genuine and fake identities [1]. However, there are serious privacy and security issues associated with the centralized gathering of such identity information.

Federated learning represents a solution to distributed learning in the form of local training and model updates exchanged for collaborative learning [2]. There is also privacy-preserving federated learning that can overcome the risks of sensitive data exposure; however, there is always a possibility of privacy or security threats due to model updates and aggregation [4]. The significance of using multiple identity characteristics is demonstrated in the context of multimodal identity verification, in which biometric and behavioral data can be complementary in detecting anomalies [3]. In distributed identity environments, federated learning is possible to help in collaboration without directly exchanging identity data [5]. But heterogeneous client data, non-independent distribution of data, communication limitations, and adversarial activity should be considered in the problem of reliable federated anomaly detection [6].

The objective of this research is to design a federated deep learning technique for privacy-aware digital identity anomaly detection in distributed systems. The study intends to facilitate collaboration in analyzing digital identities without exchanging the actual identity information among the nodes participating in the distributed system. The motivation behind this work is due to privacy concerns, heterogeneity of the distribution of data, and complexities of digital identity anomalies. The objectives of this study are designing the federated learning framework, implementing a novel anomaly detection technique, maintaining privacy while performing collaborative learning, and evaluating the performance of the technique with appropriate classification measures. This work introduces a secure and distributed method of detecting identity anomalies.

*Corresponding author. Email: danel_rdanel@outlook.com

2. RELATED WORK

There is much literature related to privacy-preserving distributed learning considering the rising need for analyzing sensitive data in a distributed environment. The current research has examined federated optimization, privacy preservation, anomaly detection, heterogeneous clients' data, and secure collaboration of learning. The use of deep learning for identity and fraud detection has been studied, showing the importance of learning complicated patterns based on behavior and transactional data. Nevertheless, there are still some issues that need to be solved concerning non-IID data, heterogeneous clients, privacy leakage, malicious clients, and anomaly detection. This literature can serve as a basis for further research on the topic under discussion.

Li et al. explored federated optimization in heterogeneous networks and statistical conditions and concluded that non-IID data from clients may greatly influence convergence and motivated solutions like FedProx [7]. Suman Kumar Sanjeev Prasanna researched self-supervised learning techniques to detect synthetic identity and proved that representation learning is capable of detecting anomalous identity features when there is a lack of labeled data [8]. Karimireddy et al. created SCAFFOLD and observed that the control of client drift may be beneficial for federated optimization under a heterogeneous distribution of data [9]. The research conducted by Suman Kumar Sanjeev Prasanna on federated identity analysis revealed that privacy-preserving collaboration enables synthetic identity detection in isolated institutional data [10]. Man et al. proposed a federated deep-learning intrusion detection technique for edge-assisted IoT architectures and proved that federated learning can be applied for network security [11]. Saha et al. analyzed privacy-preserving federated learning approaches and concluded that differential privacy, secure computation, and encryption are key mechanisms to minimize information leakage [12]. The identity analysis by graphs is implemented in relational anomaly detection [13].

In their study of privacy-preserving anomaly detection in IoT systems, Kasula et al. demonstrated that grouped federated learning could help to enhance the collaborative process of anomaly detection by minimizing data exposure [14]. The work of Kadhe et al. on privacy-preserving federated learning for the purpose of financial anomaly detection proved that collaboration between vertically and horizontally partitioned datasets could contribute to anomaly detection without exposing sensitive records [15]. In addition, Tumma et al. found that privacy and robustness continue to be related issues in federated learning since client updates might leak sensitive information or exhibit malicious behavior [16]. Generally, the literature review indicates considerable promise for using federated learning, deep representations, and privacy-preserving techniques for anomaly detection purposes.

The current body of literature suffers from limitations such as dealing with non-IID datasets, diverse network settings, privacy breaches, high communication costs, insufficient labeled identity datasets, and susceptibility to malicious updates of clients. Most of the literature evaluates federated learning for general anomaly or intrusion detection purposes without focusing on the problem of identity anomalies in the distributed networks. The proposed research is an attempt to overcome these issues by adopting a privacy-preserving federated deep learning methodology that facilitates collaboration on identity anomaly detection.

3. METHODOLOGY

This methodology describes a systematic process for the identification of digital identity anomalies while ensuring privacy in a distributed system. In this study, first, dataset collection and preprocessing are done. Next, the development of the local deep learning model at the client side takes place. Then federated learning is performed for training the model without exposing any raw identity data. Further, privacy techniques and anomaly detection methods are employed to enhance the security of the distributed learning process. Finally, the trained model is evaluated using standard classification metrics to assess its effectiveness and reliability.

3.1 Dataset and Data Preparation

The data used in the study involves a digital distributed identity dataset that includes identity attributes, behaviors, transactions, authentication activities, and network interactions. This dataset is split across different simulated network clients, symbolizing different decentralized organizations or service providers. The preprocessing of the data involves deleting duplicate entries, dealing with missing values, converting categorical attributes into numeric form, and normalizing numeric variables. Imbalance in the classes within the dataset is resolved through balancing of the training sets without affecting the independent test data. The split dataset consists of the training, validation, and test subsets.

3.2 Local Deep Learning Model

The local machine learning algorithm is constructed for each contributing client to discover intricate associations from locally available identity records. The algorithm includes input, fully-connected, nonlinear activation, dropout, and output layers. The input layer provides normalized identity characteristics, and the hidden layers generate distinctive

representations related to legal and illegal behavior of identities. The output layer returns the probability of all identity categories. The local objective function can be formulated as:

$$Lk = -\frac{1}{nk} \sum_{i=1}^{nk} yi \, log(\hat{y}i) \quad (1)$$

where nk represents the number of samples at client k, yi represents the actual class, and y^i denotes the predicted probability.

3.3 Federated Collaborative Training

Local trained models collaborate in federated learning without exchanging their raw personal data in the central server. In each round of training at the local machine, the model parameters are sent to the aggregation server, which combines all the parameters based on the contribution of individual clients to form an updated global model. The process of federated aggregation is represented by:

$$\boldsymbol{\theta^{t+1}} = \sum_{k=1}^{K} \frac{nk}{N} \theta_k^t \quad (2)$$

where θkt denotes the local parameters of client k, nk is its training-sample count, and N represents the total number of training samples. The updated model is returned to participating clients for subsequent training rounds.

3.4 Privacy and Anomaly Detection

The feature of privacy preservation is implemented using the original identity information in the client's environment. In collaborative learning, only the information necessary for parameter aggregation, that is, model information, is transmitted between the clients and the central coordinator. Extra privacy preservation can also be achieved using update clipping and noise addition to minimize the risk of reconstruction of any personal information from the exchanged parameters. The trained global model is then used on the local identity records in order to detect abnormal behavior patterns. The identities are categorized depending on their representations and probability predictions.

3.5 Performance Evaluation

Finally, the global model is assessed with the help of an independent testing dataset with both normal and anomalous identities. Accuracy, precision, recall, F1-score, and the area under the curve of the receiver operating characteristic are used for measuring the performance of the models. In addition, the confusion matrix is also used for determining the false positives and false negatives. Comparison between the federated and non-federated or traditional machine learning methods is performed to assess the effectiveness of the federated method. In addition, convergence of the model during each communication round is also assessed as a measure of training performance.

4. RESULTS

Results are presented that assess the effectiveness of the suggested federated deep learning architecture in detecting anomalies in digital identities with privacy preservation. The analysis is carried out to estimate classification performance among different models as well as improvement of performance as a result of consecutive federated communication rounds.

TABLE I. CLASSIFICATION PERFORMANCE

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Logistic Regression	89.42	87.96	88.31	88.13
Random Forest	93.67	92.84	93.21	93.02
XGBoost	95.18	94.72	94.86	94.79
CNN	96.43	95.87	96.12	95.99
Proposed Federated Deep Learning	98.76	98.42	98.61	98.51

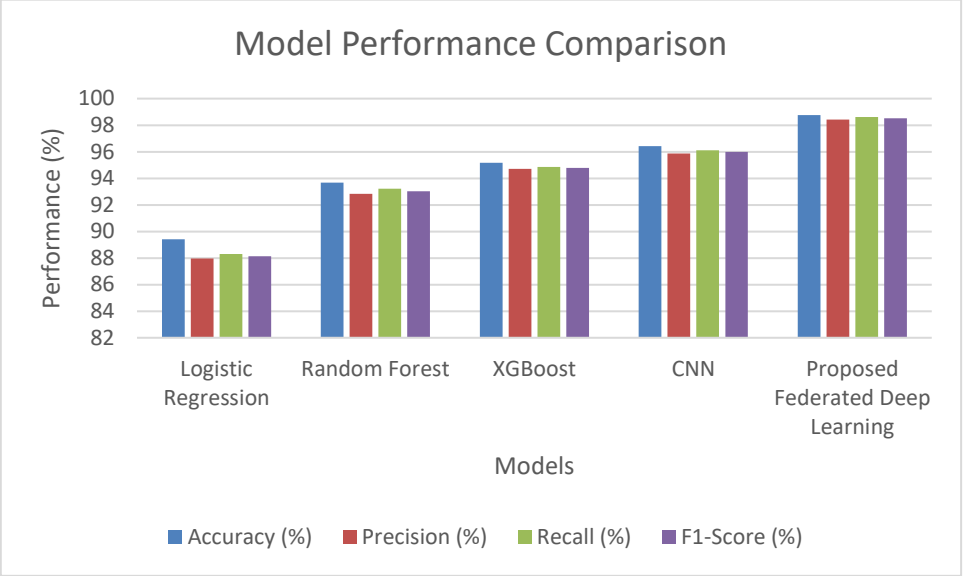

Fig. 1. Model Performance Comparison

Table 1 and Figure 1 show the comparison between the performances of the traditional machine learning model and the deep learning model for digital identity anomaly detection. It is seen that the Logistic Regression model shows the worst performance, and Random Forest and XGBoost show better classification performance. CNN gives better performance because of complex pattern recognition through learning identity characteristics. The Federated Deep Learning model gives the best performance with an accuracy of 98.76%, precision of 98.42%, recall of 98.61%, and F1-score of 98.51%. This indicates that the proposed technique is effective in detecting anomalous identities with better classification performance. The balanced precision and recall values further demonstrate reliable detection with comparatively limited false-positive and false-negative classifications.

TABLE II. FEDERATED TRAINING PERFORMANCE

Communication Round	**Training Accuracy (%)**	**Validation Accuracy (%)**	**Detection Rate (%)**
10	91.35	89.84	88.72
20	94.28	92.76	91.63
30	96.17	94.91	94.38
40	97.82	96.43	96.27
50	**98.76**	**97.68**	**98.21**

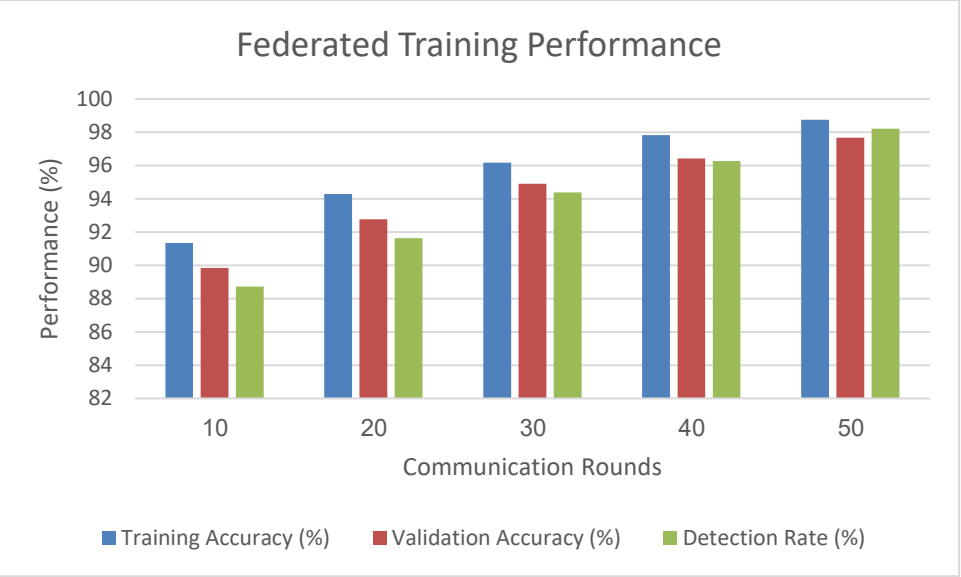

Fig. 2. Federated Training Performance

The performance of the federated learning algorithm for different numbers of communication rounds has been shown in Table 2 figure 2. The results indicate that the training accuracy, validation accuracy, and detection rate increase as more rounds of communication are performed. In ten rounds of communication, the accuracy of training and detection rates become 91.35% and 88.72%, respectively. The performances increase for 20, 30, and 40 rounds of communication. At 50 rounds of communication, the training and detection rates become 98.76% and 98.21%, while the validation accuracy becomes 97.68%.

5. DISCUSSION

The findings suggest that the federated deep learning framework that was suggested is an effective means of digital identity anomaly detection in distributed networks. In particular, the high values of the accuracy, precision, recall, and F1-score suggest strong classification ability in comparison with traditional approaches to learning. Moreover, the gradual increase of the quality metrics during communication rounds proves the positive effect of collaborative training on the learning process of representative digital identity patterns. Additionally, the suggested approach allows ensuring privacy through non-disclosure of identity data during direct transmission of unprocessed information.

6. CONCLUSION

A federated deep learning approach for privacy-preserving digital identity anomaly detection has been developed as part of this study. This method incorporates local deep learning, federated collaborative learning, privacy protection, and anomaly classification in order to solve the problems related to decentralized identity analysis. The findings show improved classification efficiency and learning progress during federated learning iterations. This system shows the possibility of collaboration without the need for data exchange in the form of identity records. The present study lays the foundation for future research in this area in terms of adaptive aggregation, privacy protection mechanisms, heterogeneous client settings, and real-life implementation.

Conflicts of Interest

The authors declare no conflicts of interest.

Funding

No external funding was received for this research.

Acknowledgment

The authors acknowledge the support and resources provided for completing this research.

References

[1] S. Kumar Sanjeev Prasanna, "IdenTransformer: A foundation model architecture for robust digital identity verification," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 13, no. 1, pp. 639–647, 2025.
[2] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Proc. 20th International Conference on Artificial Intelligence and Statistics*, vol. 54, pp. 1273–1282.
[3] S. Kumar Sanjeev Prasanna, "DeepFusion: A unified latent framework for cross-modal biometric and behavioral integrity verification," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 11, no. 1s, pp. 285–295, 2023.
[4] X. Yin, Y. Zhu, and J. Hu, "A comprehensive survey of privacy-preserving federated learning: A taxonomy, review, and future directions," *ACM Computing Surveys*, vol. 54, no. 6, Art. no. 131, pp. 1–36.
[5] S. Kumar, S. Prasanna, and L. Vantalia, "Deep learning approaches for synthetic identity detection: Models, challenges, and emerging trends," *Journal of Electrical Systems*, vol. 19, no. 3, pp. 230–243, 2023.
[6] S. Gore, D. Jadhav, M. E. Ingale, S. Gore, and U. Nanavare, "Leveraging BERT for next-generation spoken language understanding with joint intent classification and slot filling," in *Proc. 2023 International Conference on Advanced Computing Technologies and Applications (ICACTA)*, Oct. 2023, pp. 1–5.
[7] T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, "Federated optimization in heterogeneous networks," *Proceedings of Machine Learning and Systems*, vol. 2, pp. 429–450, 2020.
[8] S. Kumar Sanjeev Prasanna, "SelfSuper-ID: Self-supervised deep learning for synthetic identity detection under extreme label sparsity," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 9, no. 1, pp. 164–174, 2021.
[9] S. P. Karimireddy, S. Kale, M. Mohri, S. Reddi, S. Stich, and A. T. Suresh, "SCAFFOLD: Stochastic controlled averaging for federated learning," in *Proc. 37th International Conference on Machine Learning*, 2020, pp. 5132–5143.
[10] S. Kumar Sanjeev Prasanna, "Fed-ID: A privacy-preserving federated learning framework for cross-institutional synthetic identity discovery," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 23s, pp. 4238–4246, 2024.
[11] D. Man, F. Zeng, Y. Yang, Y. Wu, J. Miao, J. Lv, and J. Wang, "Intelligent intrusion detection based on federated learning for edge-assisted Internet of Things," *Security and Communication Networks*, vol. 2021, Art. no. 9361348, 2021.
[12] S. Saha, A. Hota, A. K. Chattopadhyay, A. Nag, and S. Nandi, "A multifaceted survey on privacy preservation of federated learning: Progress, challenges, and opportunities," *Artificial Intelligence Review*, vol. 57, Art. no. 184, 2024.
[13] S. Kumar Sanjeev Prasanna and X. Ruan, "Graph-ID: Inductive graph neural networks for high-fidelity relational anomaly detection in digital interaction networks," *Journal of Computational Analysis and Applications*, vol. 28, no. 4, pp. 72–82, 2020.
[14] V. K. Kasula, C. Tumma, and B. Konda, "A comprehensive review of artificial intelligence models for lifetime value optimization," in *Proc. 2025 2nd International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE)*, May 2025, pp. 1–5.
[15] S. R. Kadhe, H. Ludwig, N. Baracaldo, A. King, Y. Zhou, K. Houck, A. Rawat, M. Purcell, N. Holohan, M. Takeuchi, R. Kawahara, N. Drucker, and H. Shaul, "Privacy-preserving federated learning over vertically and horizontally partitioned data for financial anomaly detection," 2023.
[16] C. Tumma, R. Azmeera, S. Ayyamgari, and B. Y. R. Thumma, "Data security and privacy protection in artificial intelligence models: Challenges and defense mechanisms," *International Journal of Scientific Research in Engineering and Management*, vol. 9, pp. 1–9, 2025.