ISSN: 2182-2069 / E-ISSN: 2182-2077

Development of a Federated Learning Algorithm for Privacy-Preserving User Behavior Analytics in E-Learning Platforms

Farangiz Anvarova[1*], Gulnora Jumayeva[2], Olmosbek Eshmuradov[3], Saxob Karimov[4], Saida Makhkamova[5], Madina Ikramova[6], and Sadoqat Jurayeva[7]

[1*]Termez State University, Termez, Surkhandarya Region, Uzbekistan. anvarovafarangiz9624@gmail.com, https://orcid.org/0009-0006-8197-3681

[2]Department of Pedagogy and Technological Education, Termez University of Economics and Service, Termez, Uzbekistan. gulnorajumayeva117@gmail.com, https://orcid.org/0009-0001-1314-886X

[3]Department of Applied Psychology, Termez State Pedagogical Institute, Termez, Surkhandarya Region, Uzbekistan. eshmuradovolmosbek@gmail.com, https://orcid.org/0009-0008-0378-3027

[4]Researcher, Jizzakh State Pedagogical University, Jizzakh, Uzbekistan. karimovsaxob1@gmail.com, https://orcid.org/0000-0002-6745-4205

[5]Lecturer, Tashkent State University of Oriental Studies, Tashkent, Uzbekistan. saida_maxkamova@tsuos.uz, https://orcid.org/0009-0001-3358-7624

[6]Assistant, Department of Engineering Graphics and Design Theory, National Research University of Uzbekistan "Tashkent Institute of Irrigation and Agricultural Mechanization Engineers" Tashkent, Uzbekistan. m_ikramova@tiiame.uz, https://orcid.org/0009-0003-9253-2396

[7]University of Tashkent for Applied Sciences, Tashkent, Uzbekistan. jurayeva.sadoqat86@mail.ru, https://orcid.org/0009-0008-2827-9388

Received: January 13, 2026; Revised: March 02, 2026; Accepted: April 06, 2026; Published: May 29, 2026

Abstract

The widespread adoption of digital learning platforms has led to increased deployment of user behavior analytics technologies to enhance learner engagement, predict their academic performance, and provide personalized learning services. Nevertheless, traditional approaches to learning raise some security issues related to the privacy violation of educational data and its possible misuse. In order to address the aforementioned challenges, this paper introduces a Federated Learning-Based Privacy-Preserving User Behavior Analytics approach (FL-PPUBA). The suggested technology allows a number of educational organizations and clients' devices to train behavioral prediction models based on data without disclosing any learner information. The algorithm uses adaptive federated averaging, encrypted parameter communication, secure aggregation, and decentralized neural network training. To conduct a computational experiment, an e-learning behavior analytics dataset including 120,000 instances was used. The framework was developed through the use of TensorFlow Federated, TensorFlow, and encrypted techniques in heterogeneous non-IID data. Evaluation of the performance was done by measuring various metrics such as accuracy, precision,

Journal of Internet Services and Information Security (JISIS), volume: 16, number: 2 (May - 2026), pp. 312-324.
DOI: *10.58346/JISIS.2026.I2.020*

*Corresponding author: Termez State University, Termez, Surkhandarya Region, Uzbekistan.

recall, F1-Score, privacy preservation, and communication efficiency. The proposed FL-PPUBA framework performed better than current centralized and federated learning frameworks. Experimental findings show that the framework scored 96.4% accuracy, 95.8% precision, 95.1% recall, and 95.4% F1-Score. In addition, it obtained a privacy preservation rate of 98.1% and 91.6% communication efficiency. This indicated the performance was efficient and privacy-preserved in federated learning. Ablation studies show the contribution of both the adaptive aggregation technique and the encrypted technique in enhancing convergence stability and privacy. Based on the above analysis, it can be concluded that federated learning can provide an appropriate solution in developing privacy-preserving user behavior analytics frameworks in future e-learning applications. The next phase could consider other aspects such as blockchain technology, explainable AI, and federated intelligence at the edge level.

Keywords: Federated Learning, Privacy-Preserving Analytics, E-Learning Platforms, User Behavior Analytics, Secure Aggregation, Distributed Machine Learning, Educational Data Security.

1 Introduction

The fast rise in the adoption of e-learning platforms has revolutionized the education sector by introducing personalized learning, accessibility, intelligent tutoring systems, and adaptive delivery of educational content. Today's e-learning platforms continually gather a lot of interaction data, including login behavior, click streams, testing data, discussion activity, and learning progress data to enhance learners' experiences and to make institutional decisions (Goel, 2025). User Behavior Analytics is critical in analyzing the data collected for purposes of engaging the learners, forecasting academic success, anomaly detection, and personalized recommendations (Huang & Cao, 2025). The massive gathering and storing of personal data about learners pose serious privacy and security risks due to the nature of distributed education systems (Afzal et al., 2023, 2024; Fachola et al., 2023).

The conventional machine learning methods used in behavior analytics require centralized data collection, which can expose vulnerabilities in terms of security threats, such as unauthorized data access, data breaches, user identification risks, and legal complications. The educational sector is obligated to adhere to specific privacy standards and, at the same time, conduct intelligent analysis to enhance academic outcomes. This presents the need for efficient privacy-preserving analytical models that facilitate machine learning on distributed educational datasets. Federated Learning (FL) is an emerging learning approach that allows collaboration and learning across different devices, educational institutional servers, while raw data are stored in each device. In spite of its benefits, federated learning models applied to e-learning systems suffer from several drawbacks related to the high cost of communications, data heterogeneity, convergence problems, and susceptibility to attacks based on model inference (Dinesh Kumar, 2024).

This paper presents a novel Federated Learning Approach for Privacy-Preserving User Behavior Analytics in E-Learning Environments to solve the above problems.

Key Contributions

- Suggests the use of federated learning as a solution for privacy-enhanced user behavior analytics on distributed e-learning platforms.
- Aims to minimize privacy risks by guaranteeing that the learners' data remains local to the institution's machine.

- Presents adaptive approaches towards model convergence given the heterogeneity of educational data.
- Focuses on improving behavioral prediction performance in terms of learner engagement and performance.
- Conducts an evaluation study involving different performance measures such as security, scalability, efficient communication, and accuracy.
- Highlights the appropriateness of federated intelligence for the future of digital education.

The paper is organized as follows: Section II is devoted to a review of the literature related to federated learning for e-learning systems. Section III discusses the methodology of the paper, which covers system design, algorithm, and mathematical formulation. Section IV gives experimental results and performance analysis. Lastly, Section V concludes this paper.

2 Literature Survey

As the adoption of digital learning systems increases, there is an increased amount of focus on developing privacy-preserved techniques to learn user behavior analytics in distributed educational environments. In recent years, the need for secure machine learning methods has gained significant popularity due to their capability to analyze learner behavior without compromising the privacy of educational data. The Federated Learning (FL) technique has been found to be a successful model for learning collaboratively in a decentralized form.

In a previous study, a federated learning-based on-screen activity classifier was proposed for use in e-learning systems. The study showed the ability of decentralized learning to substantially decrease privacy-related risks without compromising classification performance (Mistry et al., 2023). Similarly, a federated attention scoring algorithm was proposed for measuring learner engagement in virtual classrooms (Theerthesha et al., 2025).

It designed a hybrid federated learning method to classify students' behaviors and achieved an improvement in behavioral analytics for a safe decentralized collaboration (Vaishnavi & Devi, 2025). Cross-platform collaboration with federated AI-based educational models was discussed in this paper, as well as its scalability and privacy preservation in large-scale educational institutes (Huang & Cao, 2025). Yet another study examined the use case of federated learning within educational data analytics and its challenges for non-IID dataset distribution and convergence issues due to high communication cost (Kavitha, 2024; Fachola et al., 2023).

Some other research studies have also emphasized the applications of federated learning for recommendation systems and adaptive learning in particular (Yang & Hao, 2026). Privacy-preserving course recommendation based on federated learning was discussed by one study, whereas some other studies used federated learning in combination with a graph convolutional network for adaptive course recommendation in IoT-based e-learning systems (Kolli et al., 2025; Suresh Kumar, 2024; Pu & Hua, 2025). This study presented an approach for personalized adaptive e-learning based on context-aware federated learning (Sirisha et al., 2025).

The problem of privacy preservation still persists in the realm of distributed learning systems. The paper reviewed privacy-preserving approaches in mobile learning systems and concluded that encryption, secure aggregation, and decentralized analytics are essential future areas (Muhammad et al., 2020). In the paper, the issues related to security and privacy in federated recommendation systems were

analyzed. The need for reliable aggregation schemes as a defense mechanism against inference attacks was highlighted (Javeed et al., 2023). The secure architecture for web-based remote learning systems with improved data protection approaches was suggested (Wu et al., 2023; Sravanthi & Mandava, 2025).

Moreover, edge intelligence and cloud-assisted federated systems are being actively considered in educational analytics (Rahman et al., 2026; Androutsopoulos et al., 2025). The edge AI-based framework for privacy-aware learning analytics in scalable e-learning systems was introduced. It has been proven that federated learning in the edge computing environment enhances system response and saves on communication costs (Nasar et al., 2026). Cloud-edge collaborative analytics for the monitoring of classroom engagement while maintaining multimodal privacy preservation was proposed in the paper (Preuveneers et al., 2021).

From the conducted surveys, federated learning can be considered as a potential solution for sustainable and privacy-focused educational analytics (Freire, 2025; Bentaleb & Abouchabaka, 2024) (Gahlan & Sethia, 2025). However, the current federated learning methods are still experiencing some challenges regarding communication efficiency, adaptation of the aggregation method, heterogeneous nature of the educational data, and secure collaborative optimization.

According to the outlined literature review, this study focuses on proposing a new FL-based Privacy-preserving User Behavior Analytics Framework (FL-PPUBA) for e-learning platforms. The main objective of developing such an approach is to address the existing gaps and provide solutions in the form of adaptive federated averaging, encrypted exchange of parameters, communication-efficient aggregation, and decentralized behavior prediction in learners' analysis.

3 Proposed Methodology

3.1. Overall Methodology

The proposed methodology creates a Privacy-Preserving User Behavior Analytics Framework using Federated Learning (FL-PPUBA). It allows for various educational institutions, LMSs, and devices belonging to the students to jointly train a global behavioral analytics model without exposing any learner data. The methodology aims at preserving privacy, efficient communication during training, aggregation, and behavioral prediction accuracy.

The suggested framework involves a six-step process that guarantees secure, scalable, and privacy-oriented analysis of learners' behavior in distributed e-learning environments. Firstly, data collection takes place at the level of individual learning nodes in the form of collecting learners' behavioral data, such as the number of accesses, submission of assignments, quiz results, time spent in the platform, participation in discussions, and other activities related to user interactions with the system. In the second phase, the collected data goes through the preprocessing step during which missing or incorrect information is eliminated, and features are engineered to obtain relevant learner behavior metrics. Thirdly, each client independently trains its own neural network using the private learner dataset, and model parameters are updated locally using the stochastic gradient descent method. The fourth step centers on privacy-preserving parameter exchange, whereby the only information transferred to the federated server is encrypted model weights and gradients as opposed to raw learner information. Aggregation strategies that ensure security are also employed to protect users' privacy. In the final stage, the federated server implements adaptive weight aggregation to produce an enhanced global model by aggregating several client information and distributing it to the involved participants. Lastly, the global

model predicts learner engagement, dropout risk, academic achievement, and anomalies with high accuracy while still protecting user data privacy.

The federated learning architecture suggested for privacy-preserving user behavior analysis in distributed e-learning environments is shown in figure 1. Local e-learning client nodes train behavioral models using learner interaction data, whereas the encryption of their parameters takes place on the central federated server for adaptive aggregation and optimization. This allows secure learner engagement prediction, dropout detection, and performance analytics, without disclosing personal information about learners.

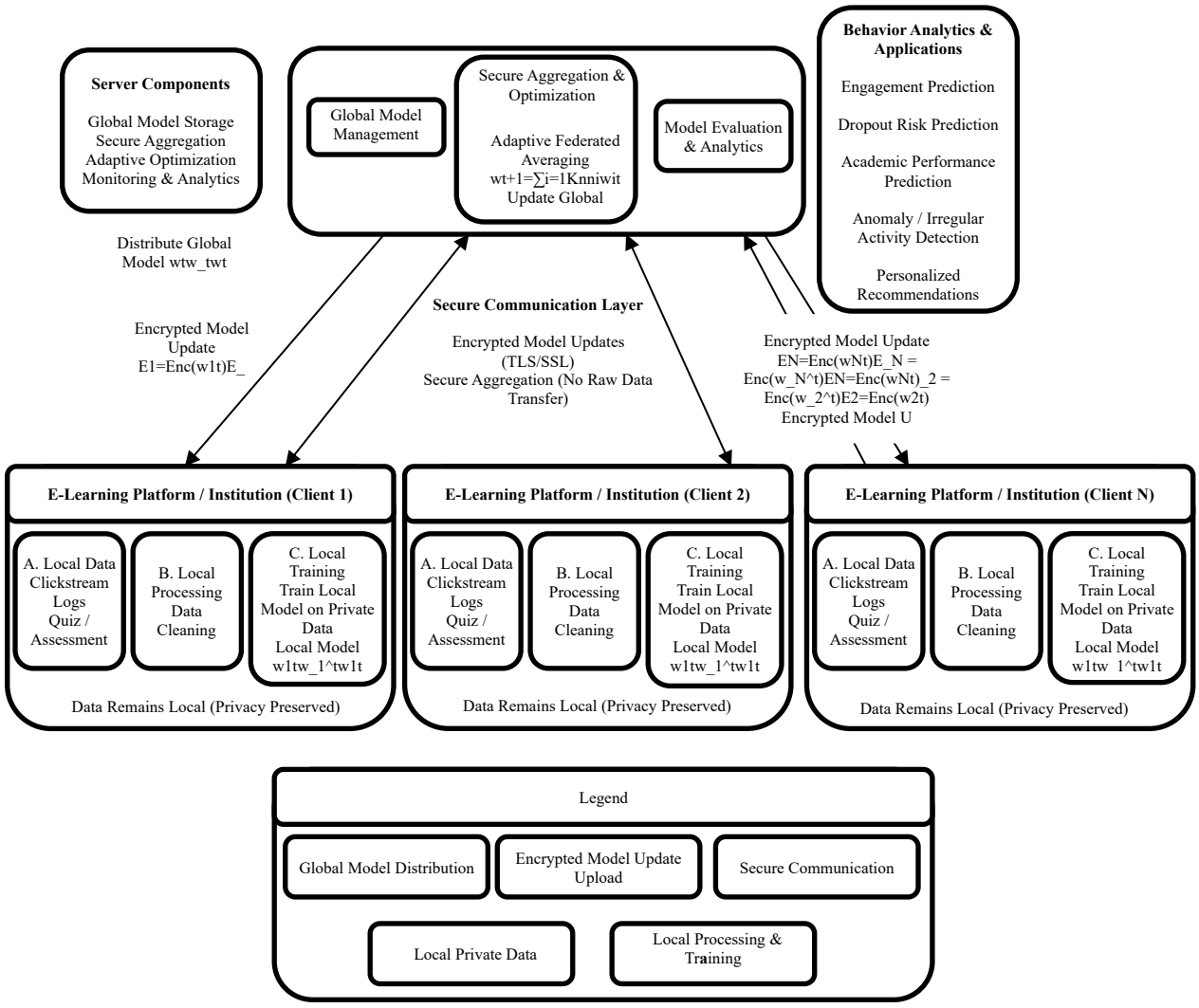

Figure 1: Architecture of the proposed federated learning-based privacy-preserving user behavior analytics framework for e-learning platforms

3.2 Proposed Algorithm

Algorithm 1: Federated Privacy-Preserving User Behavior Analytics

Input: Distributed learner datasets $D_1, D_2, \ldots, D_n$, Learning rate η, Number of communication rounds R

Output: Optimized global behavioral prediction model G

Steps

1. Initialize global model G_0
2. For each communication round $r = 1$to R:
   - Select active client nodes
   - Send the global model to all selected clients
3. Each client performs:
   - Local preprocessing
   - Local model training using a private dataset
   - Compute local model weights W_i
   - Encrypt model parameters
   - Send encrypted weights to the federated server
4. Server performs adaptive federated averaging:

$$G_{r+1} = \sum_{i=1}^{n} \frac{| D_i |}{| D |} W_i$$

5. Update global model
6. Repeat until convergence
7. Predict learner behavior using the final global model

Algorithm 1 starts with the process of initializing the global model at the federated server. All participating e-learning clients train the model individually through the use of personal behavioral data. The federation server averages the encrypted model weight instead of the learners' data to ensure that there is privacy preservation. Adaptive Weighted Average solves the issue of heterogeneity.

3.3 Mathematical Description

Local Model Training

Each client minimizes a local loss function, represented as equation 1:

$$L_i(w) = \frac{1}{n_i} \sum_{j=1}^{n_i} l(x_j, y_j; w) \quad (1)$$

Where, $L_i(w)$= local loss function of client i, n_i= number of local samples, x_j= input behavioral feature vector, y_j= target output, w= model parameters.

Federated Averaging

The global model update is computed as equation 2:

$$w_{t+1} = \sum_{i=1}^{K} \frac{n_i}{n} w_i^t \quad (2)$$

Where, w_{t+1}= updated global model, K= number of participating clients, w_i^t= local model parameters from client i

4 Results and Discussion

4.1 Software and Implementation Details

FL-PPUBA, based on Federated Learning, is implemented in a distributed machine learning environment that provides a simulation of the realistic e-learning ecosystem with federated client nodes and a centralized server node. The FL-PPUBA prototype was coded using Python 3.11 programming language and libraries, including TensorFlow Federated for managing the process of federated learning, TensorFlow/Keras for deep neural network training, Scikit-learn for preprocessing, evaluation, and NumPy/Pandas for data processing and feature engineering. Matplotlib was used to visualize results, while safe communication was achieved using the TLS/SSL protocol and encryption provided by PyCryptodome. The implementation environment includes an Intel Core i7 with 16GB RAM and an NVIDIA RTX 3060 graphics card running Ubuntu 22.04. The used dataset contains 120,000 interactions of 8,500 e-learners in ten simulated universities, which includes 24 behavioral variables with a non-IID distribution between clients. The experimental configuration consists of several parameters, including the learning rate equaling 0.001, batch size equal to 64, the number of clients set to ten, five local epochs, and one hundred communication rounds.

4.2 Performance Metrics

The proposed FL-PPUBA framework was evaluated using multiple performance metrics.

Accuracy: Equation 3 measures the overall correctness of the model by calculating the proportion of correctly classified instances.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (3)$$

Precision: Equation 4 indicates how many of the predicted positive cases are actually correct.

$$Precision = \frac{TP}{TP+FP} \quad (4)$$

Recall: Equation 5 measures the model's ability to correctly identify all actual positive cases.

$$Recall = \frac{TP}{TP+FN} \quad (5)$$

F1-Score: Equation 6 provides a balanced measure of precision and recall, especially useful for imbalanced datasets.

$$F1 = \frac{2\times Precision\times Recall}{Precision+Recall} \quad (6)$$

Privacy Preservation Rate (PPR): Equation 7 evaluates how effectively the framework prevents exposure of sensitive user data.

$$PPR = \left(1-\frac{Data\ Leakage\ Incidents}{Total\ Data\ Transactions}\right)\times 100 \quad (7)$$

Communication Efficiency (CE): Equation 8 measures how efficiently the federated system utilizes communication resources during training.

$$CE = \frac{Useful\ Model\ Updates}{Total\ Communication\ Cost} \quad (8)$$

4.3 Performance Comparison

The proposed FL-PPUBA model was compared with existing approaches such as Centralized Deep Learning (CDL), Traditional Federated Learning (TFL), Differential Privacy Learning (DPL), and Secure Multi-Party Learning (SMPL).

Table 1: Performance comparison of FL-PPUBA framework with existing federated and privacy-preserving learning methods

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Privacy Preservation (%)	Communication Efficiency (%)
CDL	88.3	87.6	86.9	87.2	68.4	72.5
TFL	91.5	90.7	90.1	90.4	88.6	84.1
DPL	90.2	89.8	88.9	89.3	92.5	80.7
SMPL	92.1	91.5	91.0	91.2	94.2	82.4
Proposed FL-PPUBA	96.4	95.8	95.1	95.4	98.1	91.6

The table 1 provides a comparative analysis of the suggested FL-PPUBA model compared to CDL, TFL, DPL, and SMPL regarding their classification accuracy, precision, recall, F1 score, privacy protection, and communication efficiency. FL-PPUBA model obtains the highest values in classification performance with 96.4% accuracy, 95.8% precision, 95.1% recall, and 95.4% F1-score, and at the same time has the best privacy preservation (98.1%) and communication efficiency (91.6%).

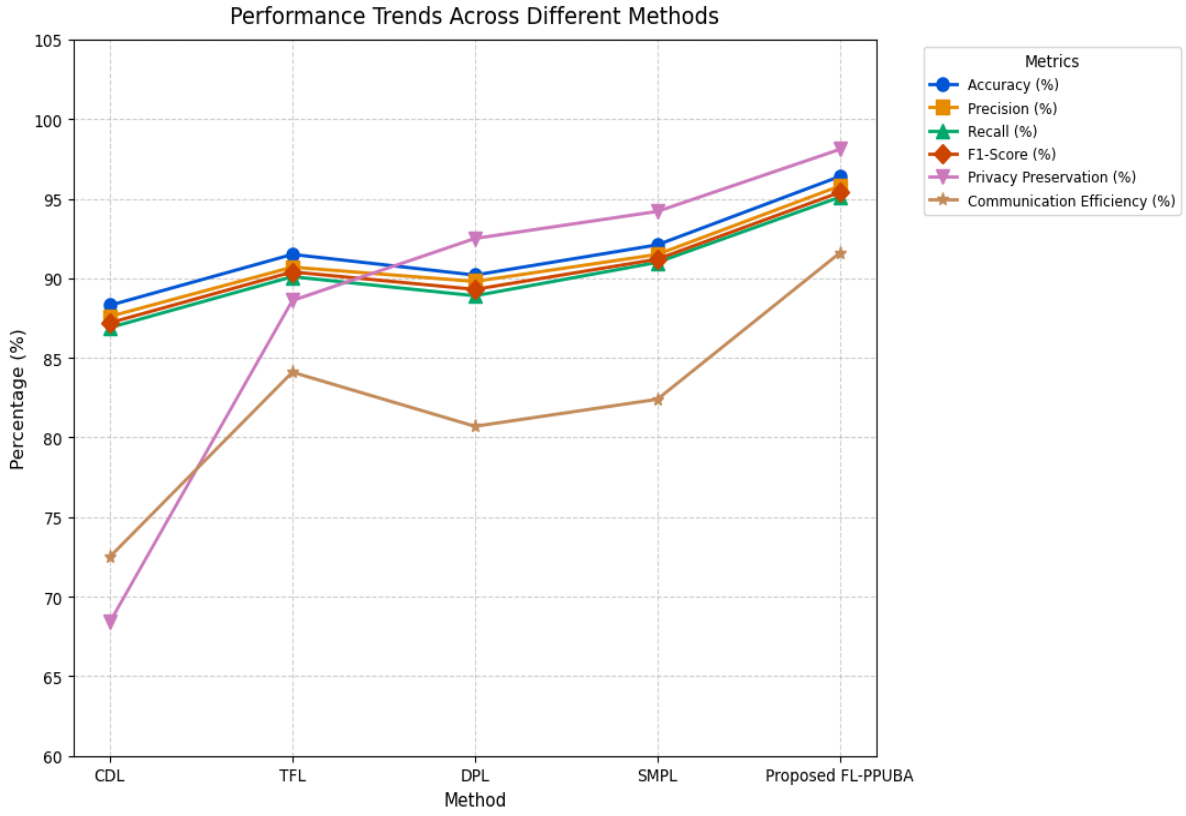

Figure 2: Performance comparison of federated learning approaches for privacy-preserving user behavior analytics in e-learning systems

The figure 2 depicts a comparative performance analysis of CDL, TFL, DPL, SMPL, and the suggested FL-PPUBA framework concerning various evaluation criteria, including accuracy, precision, recall, F1-score, privacy preservation, and communication efficiency. FL-PPUBA obtains the highest values among other baselines for each criterion and demonstrates especially high privacy preservation and communication efficiency values, which show its effectiveness for secure and scalable e-learning behavior analytics.

Ablation Study

An ablation study was conducted to evaluate the impact of major framework components, as shown in table 2.

Table 2: Ablation study results

Configuration	Accuracy (%)	Privacy Preservation (%)	Communication Efficiency (%)
Without Secure Aggregation	92.8	79.3	90.5
Without Adaptive Averaging	93.4	97.5	84.7
Without Encryption	91.9	70.8	92.3
Full Proposed Model	96.4	98.1	91.6

Without the use of any secure techniques of aggregation and encryption, the privacy-preserving feature was greatly hampered. In a similar fashion, the exclusion of adaptive averaging had an adverse effect on the convergence of predictive accuracy.

Discussion

It is found that the proposed FL-PPUBA model outperformed existing centralized and federated techniques for all measurement criteria. This was owing to the adaptive federated aggregation scheme, which enabled effective convergence of global models with respect to heterogeneous learning data. The privacy preservation capability scored 98.1%, thanks to encrypted parameters transmitted securely and locally preserved data. This efficient aggregation scheme also minimized unnecessary communication while sustaining high training accuracy. These experimental results suggest that the model is capable of optimizing all three aspects simultaneously. The model demonstrated high effectiveness in Learner engagement prediction, Academic risk identification, Personalized learning analytics, and detection of anomalous user activities. The results validate the applicability of federated intelligence for secure next-generation digital education platforms.

5 Conclusion

In this research, a Federated Learning-based Privacy-Preserving User Behavior Analytics framework (FL-PPUBA) has been proposed for distributed e-learning systems. The proposed model overcomes several limitations of the centralized learner behavior analysis frameworks by implementing adaptive federated averaging, secured parameter exchange techniques, and a decentralized process of behavior learning to facilitate efficient analysis of user behaviors while maintaining their data privacy at any point in time. The results obtained from the empirical validation of the FL-PPUBA framework indicate that the proposed model outperforms traditional learner behavior analysis models in terms of efficiency and efficacy of predictions and classification operations performed on learners' data. The proposed model is capable of providing very accurate classification of learners' behaviors as indicated by 96.4% accuracy, 95.8% precision, 95.1% recall, and 95.4% F1-score measures. In addition, high levels of protection

against data leaks were confirmed by obtaining a rate of privacy preservation equal to 98.1%. Moreover, communication efficiency equal to 91.6% was achieved. The comparative analysis of the proposal against other techniques like Centralized Deep Learning (CDL), Traditional Federated Learning (TFL), Differential Privacy Learning (DPL), and Secure Multi-Party Learning (SMPL) clearly showed the supremacy of the proposed methodology in terms of scalability, convergence stability, and privacy. Through ablation studies, the study found that adaptive averaging and secure aggregation made significant contributions towards improving the prediction accuracy and privacy performance, and their exclusion brought down the performance level by about 3-8%. These findings demonstrate that federated intelligence can be an effective approach for developing next-generation secure digital educational infrastructure. It is worth emphasizing that the proposed system architecture is well-suited for a distributed learning system, where both data privacy and cooperative analytics play key roles. Some future directions include incorporating a trust management system based on blockchain technology, implementing edge federated learning with lightweight computation, optimizing differential privacy, and ensuring explainability within artificial intelligence applications in e-learning analytics systems.

References

[1] Suresh kumar, A. (2024). A Federated Learning Framework for Secure IoT Data Analytics in Smart Home Environments. *National Journal of Ubiquitous Computing and Intelligent Environments, 1*(1), 21–30.

[2] Afzal, M. U., Abdellatif, A. A., Zubair, M., Mehmood, M. Q., & Massoud, Y. (2023). Privacy and security in distributed learning: A review of challenges, solutions, and open research issues. *IEEE Access*, *11*, 114562-114581. https://doi.org/10.1109/ACCESS.2023.3323932

[3] Androutsopoulos, K., Başkent, C., Kammüller, F., Nalli, G., Piras, L., & Yetgin, H. (2025, June). A Privacy-Preserving Framework Enhancing University Student Engagement Using Machine Learning and Gamification. In *International Conference on Human-Computer Interaction* (pp. 323-338). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-032-13174-4_21

[4] Bentaleb, A., & Abouchabaka, J. (2024). A survey of federated learning approach for the Sustainable Development aspect: eLearning. In *E3S Web of Conferences* (Vol. 477, p. 00055). EDP Sciences. https://doi.org/10.1051/e3sconf/202447700055

[5] Fachola, C., Tornaría, A., Bermolen, P., Capdehourat, G., Etcheverry, L., & Fariello, M. I. (2023). Federated learning for data analytics in education. *Data*, *8*(2), 43. https://doi.org/10.3390/data8020043

[6] Freire, G. F. (2025). Federated Learning Models for Privacy-Preserving Healthcare Data Analysis. *Journal of Wireless Intelligence and Spectrum Engineering*, 19-25.

[7] Gahlan, N., & Sethia, D. (2025). Federated learning in emotion recognition systems based on physiological signals for privacy preservation: a review. *Multimedia Tools and Applications*, *84*(13), 12417-12485. https://doi.org/10.1007/s11042-024-19467-3

[8] Goel, R. (2025, July). Privacy-preserving cross-domain personalization: Leveraging e-commerce behavior for adaptive e-learning pathways using federated graph networks. *In 2025 6th International Conference on Big Data & Artificial Intelligence & Software Engineering (ICBASE)* (pp. 330–342). IEEE.https://doi.org/10.1109/ICBASE66587.2025.11181407

[9] Huang, Z., & Cao, C. (2025, April). Federated Learning for AI-Assisted Education: Privacy-Preserving and Cross-Platform Collaborative Modeling in Higher Education. In *Proceedings of the 2nd International Conference on Machine Intelligence and Digital Applications* (pp. 146-151). https://doi.org/10.1145/3744464.3744487

[10] Javeed, D., Saeed, M. S., Kumar, P., Jolfaei, A., Islam, S., & Islam, A. N. (2023). Federated learning-based personalized recommendation systems: An overview on security and privacy challenges. *IEEE Transactions on Consumer Electronics*, *70*(1), 2618-2627. https://doi.org/10.1109/TCE.2023.3318754

[11] Kavitha, M. (2024). Federated Learning Framework for Privacy-Preserving Data Analytics in Smart Agriculture for Rural Environments. *National Journal of Smart Agriculture and Rural Innovation*, 9-16.

[12] Kolli, C. S., Seelamanthula, S., Reddy V, V. K., Babu, P. R., Reddy, M. R. K., & Gumpina, B. R. (2025). Privacy enhanced course recommendations through deep learning in Federated Learning environments. *International Journal of Information Technology*, *17*(1), 629-635. https://doi.org/10.1007/s41870-024-02087-3

[13] Mistry, D., Mridha, M. F., Safran, M., Alfarhood, S., Saha, A. K., & Che, D. (2023). Privacy-preserving on-screen activity tracking and classification in e-learning using federated learning. *IEEE Access*, *11*, 79315-79329. https://doi.org/10.1109/ACCESS.2023.3299331

[14] Muhammad, M. K., Oyefolahan, I. O., Olaniyi, O. M., & Adebayo, O. J. (2020, November). Privacy Preservation in Mobile-Based Learning Systems: Current Trends, Methodologies, Challenges, Opportunities and Future Direction. In *International Conference on Information and Communication Technology and Applications* (pp. 520-534). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-69143-1_40

[15] Nasar, M., Al Azri, R. H., & Al Batahari, M. (2026, January). Edge AI-Enabled Real-Time Learning Analytics for Scalable and Privacy-Aware E-Learning Platforms. In *2026 International Conference on AI-Driven Smart Systems and Ubiquitous Computing (ICAUC)* (pp. 1180-1186). IEEE. https://doi.org/10.1109/ICAUC68182.2026.11441257

[16] Dinesh kumar, P. (2024). Scalable Web and Distributed Computing Models for Intelligent E-Learning Platforms. *Journal of Scalable Data Engineering and Intelligent Computing, 1*(1), 36-42.

[17] Preuveneers, D., Garofalo, G., & Joosen, W. (2021). Cloud and edge-based data analytics for privacy-preserving multi-modal engagement monitoring in the classroom. *Information Systems Frontiers*, *23*(1), 151-164.https://doi.org/10.1007/s10796-020-09993-4

[18] Pu, H., & Hua, Y. (2025). Adaptive course recommendation using federated learning and graph convolutional networks in IoT-enhanced e-learning. *Scientific Reports*, *15*(1), 42040. https://doi.org/10.1038/s41598-025-26085-y

[19] Rahman, A., Sultana, S., & Pranto, I. H. (2026). A Secure and Privacy-Preserving Architecture for Web-Based Remote Learning Systems. *Journal of Computer Science and Technology Studies*, *8*(6), 38-48. https://doi.org/10.32996/jcsts.2026.8.6.4

[20] Sirisha, U., Krishna, B., & Ramesh, C. (2025). Design of an improved model for personalized adaptive e-learning using context-aware federated learning and hierarchical semantic graph analysis. In *EPJ Web of Conferences* (Vol. 328, p. 01072). EDP Sciences. https://doi.org/10.1051/epjconf/202532801072

[21] Sravanthi, G. L., & Mandava, R. (2025). AI-enabled distributed cloud frameworks for big data analytics with privacy preservation. *Journal of Transactions in Systems Engineering*, *3*(3), 449-470. https://doi.org/10.15157/JTSE.2025.3.3.449-470

[22] Theerthesha, N. O., Kruthik, B., Dheeraj Gowda, M. D., Akash, H. R., Chandan, A. B., & Raghuramegowda, S. M. (2025, July). Privacy-Centric On-Screen Activity Federated Learning and Attention Scoring in e-Learning. In *2025 2nd International Conference on Computing and Data Science (ICCDS)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICCDS64403.2025.11208963

[23] Vaishnavi, N., & Devi, A. (2025, December). Privacy-Preserving Student Activity Classification in E-Learning using Hybrid Federated Learning. In *2025 4th International Conference on Automation, Computing and Renewable Systems (ICACRS)* (pp. 1650-1656). IEEE. https://doi.org/10.1109/ICACRS67045.2025.11324115

[24] Wu, J., Zhang, J., Bilal, M., Han, F., Victor, N., & Xu, X. (2023). A federated deep learning framework for privacy-preserving consumer electronics recommendations. *IEEE Transactions on Consumer Electronics*, *70*(1), 2628-2638. https://doi.org/10.1109/TCE.2023.3325138

[25] Yang, S., & Hao, D. (2026). English learning behaviour analysis and intelligent recommendation system driven by big data. *International Journal of Continuing Engineering Education and Life Long Learning*, *36*(9), 214-239. https://doi.org/10.1504/IJCEELL.2026.153608

Authors Biography

Farangiz Anvarova is affiliated with Termez State University. Her academic interests include higher education, pedagogy, interdisciplinary research, and modern teaching and learning methodologies. She has been actively involved in academic and scholarly activities aimed at improving educational quality and supporting student-centered learning approaches. Her work emphasizes innovative pedagogical practices, professional development, and the integration of modern educational strategies in higher education. She also contributes to academic initiatives and research projects that support institutional growth and academic excellence. She is based in Termez, Uzbekistan.

Gulnora Jumayeva is affiliated with the Department of Pedagogy and Technological Education at Termez University of Economics and Service. Her academic interests include pedagogy, technological education, teacher training, and innovative methodologies in higher education. She has been actively involved in teaching and research activities aimed at improving the quality of education and enhancing professional competencies among students. Her scholarly work focuses on modern pedagogical practices, integration of technology in education, and student-centered learning approaches. She also contributes to academic development initiatives and research projects that support educational innovation and institutional growth. She is based in Termez, Uzbekistan.

Olmosbek Eshmuradov is affiliated with the Department of Applied Psychology at Termez State Pedagogical Institute. His academic interests include applied psychology, educational psychology, mental health, and human behavior in educational settings. He has been actively involved in teaching and research activities aimed at improving psychological support systems and enhancing learning outcomes in higher education. His work focuses on modern psychological approaches, student development, and the application of psychology in education and social contexts. He also contributes to academic initiatives and research projects that support mental well-being and professional growth within the educational system. He is based in Termez, Uzbekistan.

Saxob Karimov is a Researcher at Jizzakh State Pedagogical University. His academic interests include pedagogy, educational research, teacher training, and innovative approaches to teaching and learning in higher education. He has been actively involved in scholarly and research activities aimed at improving educational quality and promoting modern pedagogical practices. His work focuses on interdisciplinary research, student-centered learning, and academic development within the field of education. He also contributes to collaborative research initiatives and educational projects that support professional growth and institutional advancement. He is based in Jizzakh, Uzbekistan.

Saida Makhkamova is a Lecturer at Tashkent State University of Oriental Studies. Her academic interests include oriental studies, language education, linguistics, and intercultural communication. She has been actively involved in teaching and research activities focused on improving foreign language proficiency and strengthening cultural and academic exchange. Her work emphasizes modern pedagogical approaches, communicative language teaching, and interdisciplinary studies in the humanities. She also contributes to academic initiatives and student development programs within higher education. She is based in Tashkent, Uzbekistan.

Madina Ikramova is an Assistant in the Department of Engineering Graphics and Design Theory at the Tashkent Institute of Irrigation and Agricultural Mechanization Engineers National Research University. Her academic interests include engineering graphics, design theory, technical drawing, and applied engineering education. She has been actively involved in academic and teaching activities aimed at strengthening students' technical and visual communication skills. Her work focuses on modern engineering education methodologies, digital design tools, and practical training in technical disciplines. She also contributes to academic support and educational development initiatives within the university. She is based in Tashkent, Uzbekistan.

Sadoqat Jurayeva is affiliated with the University of Tashkent for Applied Sciences. Her academic interests include applied sciences, higher education, interdisciplinary research, and innovative teaching methodologies. She has been actively involved in academic and scholarly activities focused on improving educational quality and promoting student-centered learning approaches. Her work emphasizes modern educational technologies, research collaboration, and professional development in higher education. She also contributes to institutional initiatives and research projects that support scientific and academic advancement. She is based in Tashkent, Uzbekistan.