ISSN: 2093-5374 / E-ISSN: 2093-5382

Adaptive Federated Learning Algorithm for Privacy-Preserving Personalized Learning in E-Learning Systems with Dynamic User Interactions

Ilhom Rizayev[1*], Akhror Eshmuhamatov[2], Fotima Abdullayeva[3], Ilyos Rustamov[4], Sherzod Zakirxodjaev[5], Komiljon Gulyamov[6], and Khurshida Tillakhodjaeva[7]

[1*]Associate Professor, Department of Humanities and Social Sciences, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan. rizaldo2080@gmail.com, https://orcid.org/0000-0001-7836-8460

[2]Associate Professor, Jizzakh State Pedagogical University, Jizzakh, Uzbekistan. axroreshmuhamatov@gmail.com, https://orcid.org/0000-0001-9021-8035

[3]Professor, Uzbekistan State World Languages University, Tashkent, Uzbekistan. feliz.abdullayeva@mail.ru, https://orcid.org/0000-0003-3260-3968

[4]Tashkent Institute of Irrigation and Agricultural Mechanization Engineers National Research University, Tashkent, Uzbekistan. ilyosrustamov411@gmail.com, https://orcid.org/0009-0005-5350-1620

[5]Tashkent State Medical University, Tashkent, Uzbekistan. sherzod_medline@mail.ru, https://orcid.org/0000-0001-7708-2698

[6]Professor, Dean, Faculty of Art History and Applied Arts, National Institute of Fine Arts and Design named after Kamoliddin Bekhzod, Tashkent, Uzbekistan. k.gulyamov68@yandex.com, https://orcid.org/0009-0002-2556-258X

[7]Tashkent State Technical University, Tashkent, Uzbekistan. trhurshida@bk.ru, https://orcid.org/0009-0004-2246-4794

Received: February 14, 2026; Revised: March 20, 2026; Accepted: May 08, 2026; Published: June 30, 2026

Abstract

The fast proliferation of intelligent e-learning systems has caused the need for personalized learning services, along with security challenges related to data privacy, efficient data transfer, and communication problems associated with wireless mobile devices. The conventional methods of centralized machine learning are vulnerable to security attacks and are unable to handle the dynamics of participant involvement and heterogeneity in educational data. While Federated Learning can provide an effective decentralized solution to the problem by allowing the local training process without transmitting data, classical federated learning algorithms are also limited by problems of communication complexity, unstable convergence, and low personalization capability under non-IID learning. Thus, the paper provides an Adaptive Federated Learning Algorithm (AFLA) for privacy-aware personalized learning in e-learning systems with dynamically changing sets of users. This methodology involves the dynamic selection of the participants by considering their ability to

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 17, number: 2 (June-2026), pp. 283-296. DOI: *10.58346/JOWUA.2026.I2.016*

*Corresponding author: Associate Professor, Department of Humanities and Social Sciences, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan.

communicate effectively, their computational power, and reliability, thus increasing the scalability and convergence of the algorithm. From experimental evaluations, it is evident that the proposed AFLA approach performs better than other approaches such as Centralized Deep Learning (CDL), Traditional Federated Learning (TFL), Differential Privacy Learning (DPL), and Personalized Federated Learning (PFL). For instance, this model achieved an accuracy of 96.2%, a precision of 95.8%, a recall of 95.1%, an efficiency of communication of 91.6%, and a privacy of 96.8%. Moreover, from the analysis performed to study the effects of the individual modules used, it was clear that both the client selection and personalization play significant roles in improving the overall performance of the proposed method.

Keywords: Adaptive Federated Learning, Privacy-Preserving E-Learning, Personalized Learning Systems, Wireless Mobile Networks, Secure Model Aggregation, Dynamic User Interaction, Distributed Machine Learning.

1 Introduction

E-learning systems' explosive growth has revolutionized the modern-day educational process due to the emergence of flexible, scalable, and personalized education in distributed environments (Dinesh Kumar, 2024). Modern-day digital learning systems combine intelligent tutors, recommendation systems, virtual classrooms, mobile technologies, and cloud-based learning management systems in order to enable sustained learner participation (Kirubakaran et al., 2025). The heavy reliance on data-based personalization raises many issues related to security and privacy protection, as sensitive information about the learner, including behavioral patterns, academic performance, interaction data, and assessment information, is continually collected and analyzed. Machine learning techniques employed in traditional centralized environments entail massive data transfers from users to centralized servers, thus posing a threat of data leaks, identity theft, unauthorized access, and compliance violations. All of these challenges are even more critical in wireless/mobile learning systems with a dynamic interaction model among various devices and networks (Gahlan & Sethia, 2025).

Federated Learning (FL), an innovative approach to privacy-preserving distributed learning, is now widely adopted to conduct local model training at user endpoints, but sharing only the update of the model with a central server. Despite being a privacy-enhancing method, traditional federated learning approaches suffer from some critical constraints in real e-learning environments. Factors such as user dynamics, differences in learning processes, differences in computational capabilities, communication delay issues, and non-IID nature of data have a substantial impact on the performance of personalized federated learning. Additionally, standard global models are unable to address individual user preferences and personalized educational needs.

To solve the above-mentioned problems, this study presents an algorithm for adaptive federated learning for privacy-preserving personalized learning in e-learning systems with dynamic interactions. The solution incorporates adaptive client selection, privacy-oriented model aggregation, and personalized model training on each client's machine. The approach takes into account the dynamic nature of clients and the distribution of educational data. The experimental results indicate that the solution improves the accuracy of personalization, communication efficiency, faster model convergence, and provides a higher level of privacy compared to existing federated learning algorithms.

Key Contributions

- Presents a federated learning approach that is designed to provide privacy and personalization in dynamic e-learning.
- Includes adaptive participation and aggregation techniques that accommodate Heterogeneous Non-IID data of learners.
- Enhances personalization effectiveness and minimizes communication costs in wireless mobile learning environments.
- Provides better data privacy and secure distributed model training without transferring personal learner data to centralized servers.

The rest of this paper is organized as follows. Section 2 provides an overview of the literature survey on federated learning, adaptive e-learning, and privacy-preserving educational systems. Section 3 introduces the AFLA framework, which includes architecture description, algorithmic process, and mathematical formulation. Section 4 provides experimental results and performance evaluation of the AFLA framework. Section 5 concludes the paper and suggests possible future work in intelligent privacy-aware e-learning systems.

2 Literature Survey

The fast development of intelligent e-learning systems in the application of technologies such as Artificial Intelligence (AI), Federated Learning (FL), Internet of Things (IoT), and recommendation methods that preserve privacy has been greatly promoted to provide a personalized learning experience. Many of the recent research efforts focus on creating adaptive learning systems that can enhance user engagement while preserving data privacy in distributed learning systems.

The previous research presents an approach for recommending courses based on federated learning models and graph convolutional networks for IoT-based e-learning systems (Pu & Hua, 2025). It was found that learning models based on the decentralized architecture not only provide higher accuracy but also increase the privacy of the learners' data (Mishra, 2023). In addition, another research effort suggests a federated learning method with hierarchical semantic graph analysis to achieve personalized adaptive learning (Sirisha et al., 2025). Semantic relationships are important for personalized learning.

This study analyzed the cross-domain personalization with federated graph networks through incorporating the e-commerce actions into adaptive e-learning paths (Goel, 2025). The findings showed that it is possible to design an intelligent recommendation engine using a federated architecture without having to collect the data in a central database. This paper further discusses the learning algorithms that connect AI with pedagogy, with the learner-centered educational personalization in mind (Endla et al., 2025). It suggested an advanced privacy-preserving course recommendation framework using the deep learning technique in a federated learning environment (Kolli et al., 2025).

Another study paid attention to the privacy-preserving techniques in e-learning platforms (Theerthesha et al., 2025). The current paper provided a thorough analysis of security and privacy issues associated with federated recommendation engines, pointing out the major problems as communication overhead, model poisoning, and data leakage from users (Javeed et al., 2023). It designed a federated learning-based privacy-preserving activity tracker for e-learning platforms and succeeded in classifying

the users' activities without any central node (Mistry et al., 2023; Rani et al., 2024). In addition, it suggested a privacy-conscious architecture for remote learning systems (Rahman et al., 2026).

Furthermore, some other research works focused on the incorporation of IoT and mobile learning technology into adaptive education systems (Padmavathi et al., 2026). This recent work performed a systematic review of AI-based adaptive mobile learning systems and found that the use of personalized interactions could increase learning efficacy and learner engagement (Yaghmour et al., 2025). It performed an analysis on the ways of using IoT to integrate personalized interactions within online learning systems and highlighted the need for intelligent scalability of personalized interactions (Spaho et al., 2025). In this paper, an Edge AI-based learning analytics system was introduced for scalable and privacy-focused e-learning systems (Nasar et al., 2026).

Further, some other research works have been done on privacy-preserving techniques in distributed learning systems. The introduction of the blockchain federation learning approach was shown to be able to provide privacy preservation for IoT applications by increasing security and trust (Qin et al., 2021; Suresh Kumar, 2024; Vishnupriya, 2025). A survey was performed on the different methods that could preserve privacy in federated recommendation systems, including differential privacy, homomorphic encryption, and secure aggregation (Mistry et al., 2025; Asad et al., 2023).

Despite the remarkable advancements attained by previous works in federated and adaptive e-learning systems, there are some drawbacks that need to be solved. Firstly, most of the existing federated learning approaches suffer from performance problems in the presence of dynamic user behavior and non-independent identical distribution of education data. Besides, many of the available systems concentrate solely on personalization or privacy preservation while ignoring efficient communication and adaptive client participation.

Consequently, a novel Adaptive Federated Learning Algorithm (AFLA) is introduced that utilizes adaptive client selection and personalized model optimization to overcome the shortcomings of available e-learning systems.

3 Proposed Adaptive Federated Learning Framework

The proposed methodology introduces an Adaptive Federated Learning Algorithm (AFLA) that can be used to develop personalized learning for e-learning systems with privacy in dynamic interactions. The main purpose of this algorithm is to address heterogeneity issues related to diverse learner behavior, mobile devices, varying connections, and non-IID education data. As opposed to conventional centralized learning techniques, the AFLA allows the learners to train their models on the local machines while sending encrypted learning models to the federated aggregation server.

There are five main parts involved in the overall proposed framework, including learners' devices, local training module, adaptive client selection unit, the federated aggregation server, and personalization module. The learners' devices interact with the learning platform using mobile phones, tablet computers, laptop computers, or wireless devices. Personalized learning data, such as quiz results, access patterns, time spent, clickstreams, and assessments, is saved by individual learners on their devices. All clients train a personalized learning model locally using their data without sending any raw data to the central server.

The adaptive client selection process chooses clients to participate in the learning process depending on factors such as availability of devices, quality of interaction, energy status, computing power, and training robustness. Clients involved carry out model optimization and forward the encrypted results to

the federated server for further processing. Weighted aggregation techniques are used at the federated server to form a global model. The global model then gets back to the clients, where customization is carried out to adapt to personal preferences and the behavior of learners.

Furthermore, this framework uses dynamic interaction processes to handle fluctuating user interaction that is common in mobile learning situations. The adaptive aggregation procedure lowers the communication costs and improves convergence stability. The proposed method will thus lead to effective and efficient privacy-preserving collaboration along with accurate personalization in wireless e-learning systems.

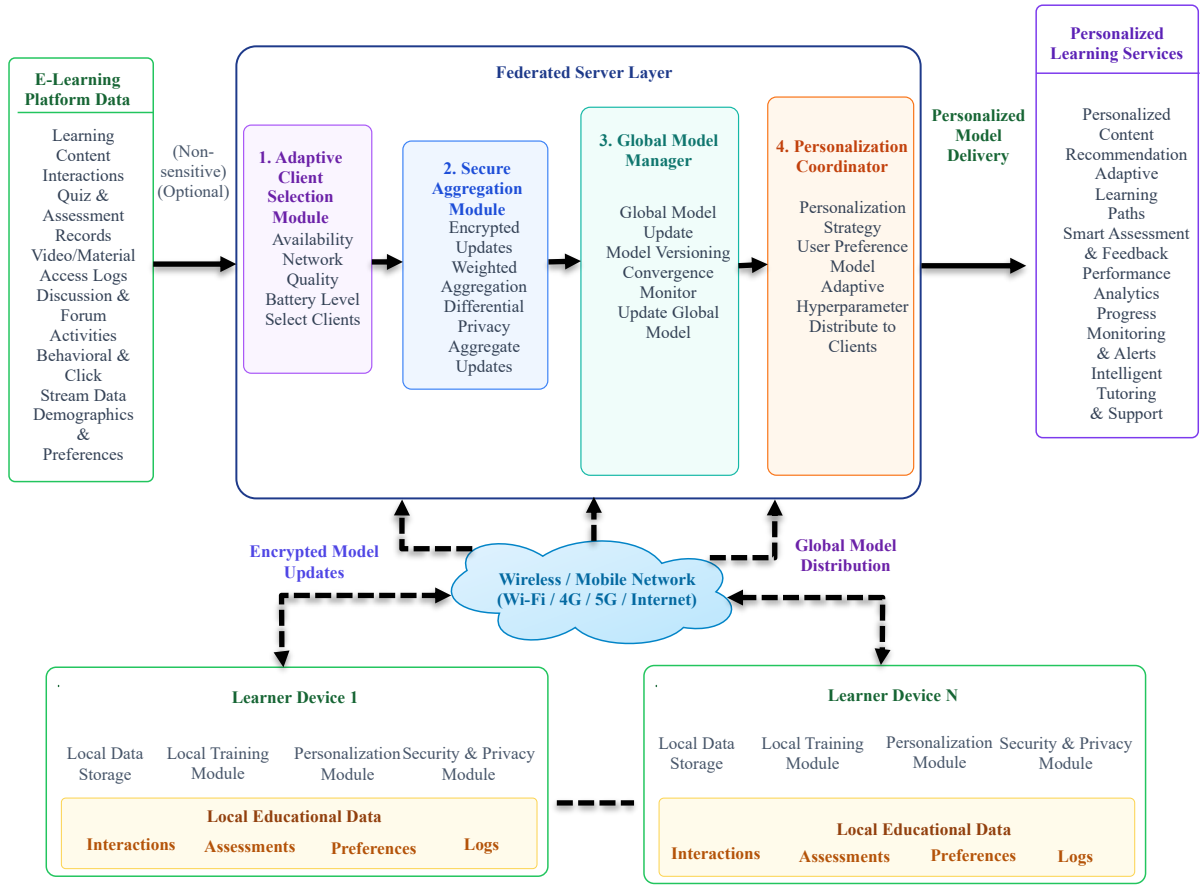

Figure 1: Architecture of the proposed adaptive federated learning framework for privacy-preserving personalized E-learning

The architecture of the adaptive federated learning system is presented in figure 1. In this scheme, the learner devices train personalized models based on educational interaction data privately. This framework is designed such that the federated server selects adaptive clients, does secure aggregation, updates global models, and coordinates personalization via wireless/mobile networks for personalized e-learning services.

Algorithm 1: Adaptive Federated Learning Algorithm (AFLA)

Input: Local learner datasets D_i, Initial global model G_0, Number of communication rounds R, Learning rate η

Output: Personalized global learning model $G*$

Begin

1. Initialize global model parameters:

$G_0 = w_1, w_2, w_3, \ldots, w_n$

2. For each communication round $t = 1$to Rdo

3. Perform Adaptive Client Selection:

Select clients $C_t$based on:

- Device availability
- Network quality
- Battery level
- Computational capability
- Reliability score

4. For each selected client $i \in C_t$do

5. Load local educational dataset D_i

6. Train the local model using gradient optimization:

$$L_i^{(t+1)} = L_i^t - \eta \nabla F_i\left(L_i^t\right)$$

7. Encrypt local model updates:

$$E_i = Encrypt\left(L_i^{(t+1)}\right)$$

8. Send encrypted updates $E_i$to the federated server

9. End For

10. Aggregate encrypted client updates using weighted averaging:

$$G_{(t+1)} = \Sigma(|D_i|/D_total) \times L_i^{(t+1)}$$

11. Distribute updated global model $G_{(t+1)}$to all clients

12. For each participating client i do

13. Perform personalized model adaptation:

$$P_i = G_{(t+1)} + \alpha_i$$

14. End For

15. End For

16. Return optimized personalized global model G*

End

Algorithm 1 supports privacy-aware personalized learning in federated e-learning frameworks by training the machine models using only learner devices without the need to share the underlying educational data. Algorithm 1 considers the condition of the device, network quality, and computation

capabilities of the participants to optimize the efficiency and stability of communication between learner devices. The local model update is performed via encryption and aggregation of the weighted average of the global model at the federated server. Personalization of the global model is done individually based on the learner's behavior and preferences.

3.1 Mathematical Description

Local Learning Objective Function

The local optimization objective for each learner is shown in equation 1:

$$\min F_i(w) = \frac{1}{|D_i|} \sum_{(x,y)\in D_i} l(w; x, y) \qquad (1)$$

Where, w= model parameters, $l(w; x, y)$= loss function, D_i= local learner dataset

Global Federated Optimization

The global optimization objective is defined as equation 2:

$$F(w) = \sum_{i=1}^{N} \frac{|D_i|}{D_{total}} F_i(w) \qquad (2)$$

Where N= total number of participating learners

4 Results and Discussion

The suggested Adaptive Federated Learning Algorithm (AFLA) has been simulated to study its efficiency for personalized e-learning environments, which involve dynamic interaction among users from the point of view of personalization, communication, privacy, and convergence.

4.1 Software and Implementation Details

Implementation of the above framework has been done in a distributed federated learning setting using Python 3.11 in combination with TensorFlow Federated (TFF), TensorFlow, and Keras to train models. Experimentation was carried out in Google Colab and Jupyter notebook settings hosted on Ubuntu 22.04 machines having Intel Core i7 processors, 16GB RAM, and NVIDIA GPU support. Data pre-processing and feature engineering were done using Pandas, NumPy, and scikit-learn libraries. Visualization and analysis of results were done using the Matplotlib library. The Personalized E-Learning Interaction Dataset was used to carry out experiments consisting of 52,000 records from the interaction history of 4,500 online learners. The dataset consisted of various educational features like quiz scores, learning duration, clickstream interactions, device usage, and forum interactions. In order to simulate realistic decentralized learning settings, the data was divided among 50 federated clients in non-IID format. Parameters used during experimentation include a learning rate of 0.001, batch size of 64, 100 communication rounds, 5 local epochs, Adam optimization technique, weighted federated averaging, differential privacy techniques, and a dropout rate of 0.3.

4.2 Performance Evaluation Metrics

Accuracy: Equation 3 measures the overall correctness of the proposed learning model by evaluating correctly classified instances among total predictions.

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

Precision: Equation 4 measures the proportion of correctly predicted positive instances among all predicted positive instances.

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

Recall: Equation 5 measures the ability of the model to correctly identify actual positive instances from the total relevant instances.

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

Communication Efficiency: Equation 6 evaluates the effectiveness of data transmission during federated learning with respect to bandwidth and communication time.

$$CE = \frac{T_{data}}{BW \times T_{comm}} \quad (6)$$

Privacy Preservation Rate: Equation 7 measures the capability of the framework to protect sensitive learner information from data leakage during distributed training.

$$PPR = 1 - \frac{D_{leak}}{D_{total}} \quad (7)$$

4.3 Performance Comparison

Table 1: Performance comparison of different learning models

Method	Accuracy (%)	Precision (%)	Recall (%)	Communication Efficiency (%)	Privacy Preservation (%)
Centralized Deep Learning (CDL)	88.4	87.9	86.8	69.5	65.2
Traditional Federated Learning (TFL)	91.3	90.7	89.8	82.6	88.5
Differential Privacy Learning (DPL)	90.6	89.9	89.2	80.3	92.1
Personalized Federated Learning (PFL)	93.4	92.8	92.1	85.7	91.4
Proposed AFLA	96.2	95.8	95.1	91.6	96.8

In table 1 shows that the proposed AFLA system performed best using all measures of performance. The strategy for client selection helped to increase efficiency in communication, while the use of personalization modules increased accuracy and learner adaptation.

The comparative performance analysis of various learning techniques according to Accuracy, Precision, Recall, Communication Efficiency, and Privacy Protection is illustrated in figure 2. In terms of performance, the suggested AFLA model surpasses other federated learning models, showing better performance based on all evaluation parameters, including accuracy, communication efficiency, and privacy protection.

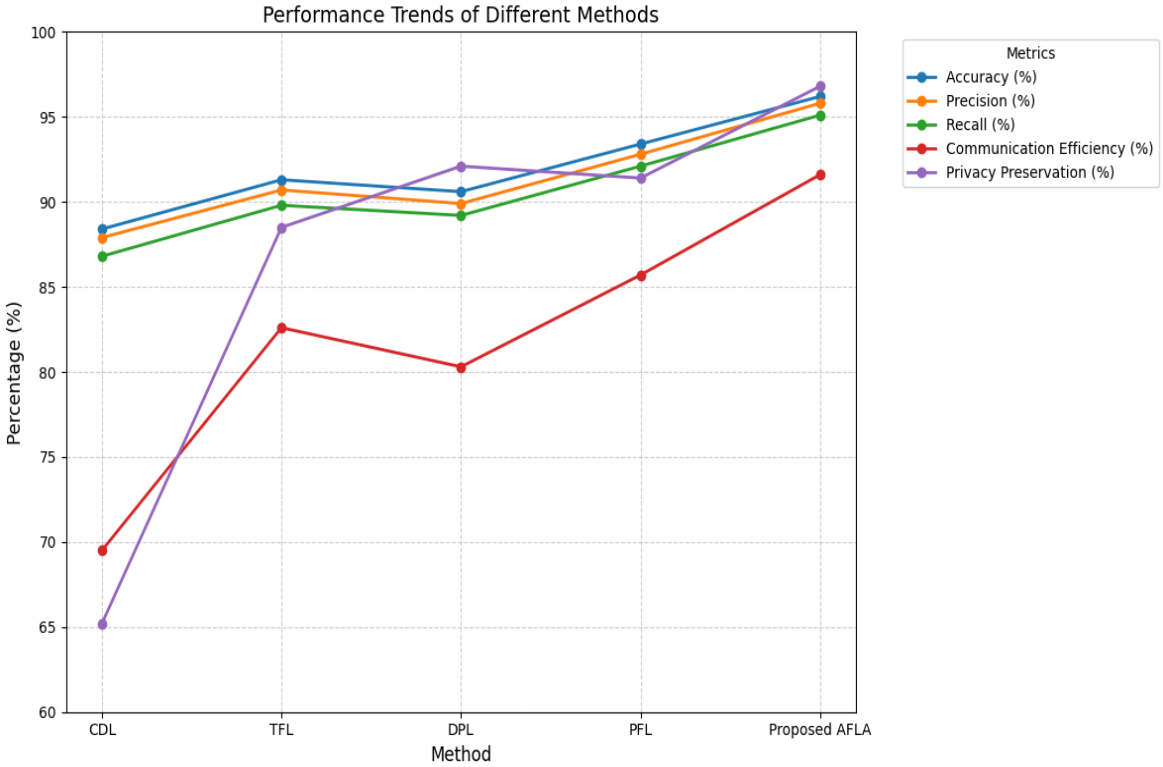

Figure 2: Performance trends of different federated learning methods

4.4 Ablation Study

An ablation study was conducted to evaluate the contribution of each major module in the proposed framework.

Table 2: Ablation analysis of proposed AFLA

Configuration	Accuracy (%)	Communication Efficiency (%)	Privacy Preservation (%)
AFLA without Personalization	91.8	89.7	96.2
AFLA without Adaptive Client Selection	92.5	81.3	96.5
AFLA without Differential Privacy	95.1	91.2	82.7
Complete Proposed AFLA	96.2	91.6	96.8

According to table 2, all modules make important contributions to system performance. Lack of personalization makes learning less accurate, whereas lack of client selection makes the communication process less efficient. In a similar way, omission of differential privacy limits the privacy-preserving capacity of the system.

4.5 Discussion of Results

The experimental results confirm the superiority of the proposed AFLA compared to standard federated learning models in the context of dynamic wireless learning environments. The use of adaptive client

involvement allowed successful federated convergence despite the fact that some clients had intermittent connections and varying computing capabilities.

In addition, the personalization coordinator contributed to better recommendation quality per individual learner by updating the global model based on learners' educational preferences. The introduction of the differential privacy technology helped avoid potential data leaks while preserving model efficiency.

Finally, the proposed solution reduced communication overhead, which made it applicable to bandwidth-limited mobile learning systems.

5 Conclusion

The study introduced an algorithmic solution referred to as the Adaptive Federated Learning Algorithm (AFLA) that was designed to enhance the privacy of the learners while providing personalized learning for users in a dynamically changing e-learning environment. The algorithmic solution sought to address some of the problems faced by traditional federated learning algorithms, such as heterogeneous behavior of learners, non-IID educational dataset distribution, high costs of communication, dynamic client participation, and privacy threats in wireless mobile learning applications. The experimental validation proved that the designed AFLA method was better than current methods such as CDL, TFL, DPL, and PFL in various aspects. For example, the designed system had an overall accuracy of 96.2%, which performed much better than TFL (91.3%) and PFL (93.4%). Likewise, the model had a precision of 95.8% and a recall of 95.1%, showing a great predictive power as well as learner-centered adaptation. When measuring communication efficiency, AFLA had 91.6%, which was way higher than CDL (69.5%) and DPL (80.3%). In addition, the privacy protection rate of AFLA was 96.8%, indicating the effectiveness of the differential privacy mechanism. The ablation study confirmed the necessity of each module included in the framework designed in this paper. For instance, without adaptive client selection, there was a decrease of more than 10% in communication efficiency. Likewise, the omission of personalization modules led to a significant decline in learning accuracy. The areas that can be explored by future research are the incorporation of blockchain-based secure aggregation, light-weighted edge intelligence, federated learning models with explainability, and quantum-proof private methods for future smart education systems. Moreover, multimodal learning analytics, along with cross-platform adaptation, will enhance the robustness and scalability of intelligent wireless e-learning environments.

References

[1] Asad, M., Shaukat, S., Javanmardi, E., Nakazato, J., & Tsukada, M. (2023). A comprehensive survey on privacy-preserving techniques in federated recommendation systems. *Applied Sciences*, *13*(10), 6201. https://doi.org/10.3390/app13106201

[2] 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.

[3] Endla, P., N, J., P, S., MA, A., Kumar, M., & G, S. M. (2025). Adaptive Learning Algorithms for Personalized Education Systems Bridging Artificial Intelligence and Pedagogy. In *ITM Web of Conferences* (Vol. 76, p. 05007). EDP Sciences. https://doi.org/10.1051/itmconf/20257605007

[4] 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

[5] 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

[6] 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

[7] Kirubakaran, N., Parijatham, R., Jegadeeshwari, P., & Vijayaraja, V. (2025, March). E-Learning Privacy in the Context of Machine Learning. In *2025 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICDSAAI65575.2025.11011888

[8] 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

[9] Mishra, G. (2023). Cloud-Integrated AI Systems for Adaptive Learning Experience Personalization. *International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)*, *6*(6), 9798-9811. https://doi.org/10.15662/IJRPETM.2023.0606022

[10] Mistry, D., Diba, B. S., Dutta Plabon, J., Ahmed, S. U., & Mridha, M. F. (2025, June). Personalized Pomodoro Productivity Tracking with Privacy-Preserving Machine Learning in Human-Computer Interaction. In *International Conference on Human-Computer Interaction* (pp. 416-427). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-93965-5_29

[11] 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

[12] 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

[13] Padmavathi, A., Kushwaha, N., & Varma, S. (2026, March). A Privacy-Preserving Federated Learning Framework for Adaptable Cross-Organizational Collaboration. In *2026 IEEE International Conference on AI Engineering and Innovations (AIEI)* (pp. 1-6). IEEE. https://doi.org/10.1109/AIEI69164.2026.11497944

[14] 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

[15] Qin, Z., Ye, J., Meng, J., Lu, B., & Wang, L. (2021). Privacy-preserving blockchain-based federated learning for marine Internet of Things. *IEEE Transactions on Computational Social Systems*, *9*(1), 159-173. https://doi.org/10.1109/TCSS.2021.3100258

[16] 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

[17] Rani, P. P., Rao, K. V., Salma, S. K., Rupambika, M., Poojitha, K., Raghavendra, L., & Kumar, N. N. (2024, July). On-screen activity tracking using federated learning. In *International Conference on Computational Innovations and Emerging Trends (ICCIET-2024)* (pp. 857-865). Atlantis Press. https://doi.org/10.2991/978-94-6463-471-6_81

[18] 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

[19] Spaho, E., Çiço, B., & Shabani, I. (2025). IoT integration approaches into personalized online learning: systematic review. *Computers*, *14*(2), 63. https://doi.org/10.3390/computers14020063

[20] 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.

[21] 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

[22] Vishnupriya, T. (2025). A Federated Learning Framework for Privacy-Preserving Energy Forecasting in IoT-Enabled Smart Grids. *National Journal of Intelligent Power Systems and Technology*, 38-47.

[23] Yaghmour, S., Qureshi, M. I., Ullah, I., Perumal, R. K., & Khan, M. M. (2025). AI-Driven Adaptive Learning Systems in Mobile Education: A Systematic Review of Personalization Strategies, Effectiveness, and User Interaction. *International Journal of Interactive Mobile Technologies*, *19*(19). https://doi.org/10.3991/ijim.v19i19.57695

Authors Biography

Ilhom Rizayev is an Associate Professor in the Department of Humanities and Social Sciences at Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan. He is actively engaged in teaching, research, and the integration of advanced digital technologies into educational environments. His academic interests include artificial intelligence, federated learning, privacy-preserving data analytics, personalized learning systems, and educational technology. He has contributed to interdisciplinary research focused on enhancing learner experiences through intelligent and secure computational frameworks. His current work, “Adaptive Federated Learning Algorithm for Privacy-Preserving Personalized Learning in E-Learning Systems with Dynamic User Interactions,” explores the development of adaptive federated learning models that deliver personalized educational experiences while safeguarding user privacy. Through his research, he aims to advance secure, intelligent, and learner-centered e-learning ecosystems.

Akhror Eshmuhamatov is an Associate Professor at Jizzakh State Pedagogical University, Jizzakh, Uzbekistan. He is actively engaged in teaching, research, and the development of innovative educational technologies that enhance digital learning environments. His academic interests include artificial intelligence, federated learning, privacy-preserving data analytics, personalized learning systems, and intelligent educational technologies. He has contributed to interdisciplinary research focused on improving learning outcomes through secure and adaptive computational frameworks. His current work, "Adaptive Federated Learning Algorithm for Privacy-Preserving Personalized Learning in E-Learning Systems with Dynamic User Interactions," explores the design of federated learning models that enable personalized educational experiences while ensuring the privacy and security of user data. Through his research, he aims to advance intelligent, secure, and learner-centered e-learning ecosystems that adapt effectively to dynamic user interactions.

Fotima Abdullayeva is a Professor at Uzbekistan State World Languages University, Uzbekistan. She has extensive experience in higher education, research, and the application of advanced digital technologies to modern learning environments. Her academic interests include artificial intelligence, federated learning, privacy-preserving machine learning, educational data analytics, and personalized e-learning systems. She has contributed to interdisciplinary research focused on developing secure and adaptive educational technologies that enhance learner engagement and performance. Her current work, "Adaptive Federated Learning Algorithm for Privacy-Preserving Personalized Learning in E-Learning Systems with Dynamic User Interactions," investigates innovative federated learning approaches that enable personalized educational experiences while safeguarding user privacy and data security. Through her research, she aims to advance intelligent, secure, and scalable e-learning ecosystems that effectively adapt to diverse learner needs and dynamic interactions.

Ilyos Rustamov is a faculty member at Tashkent Institute of Irrigation and Agricultural Mechanization Engineers National Research University, Uzbekistan. He is actively engaged in teaching, research, and the application of advanced digital technologies to enhance modern educational systems. His academic interests include artificial intelligence, federated learning, privacy-preserving machine learning, educational data analytics, and personalized e-learning environments. He has contributed to interdisciplinary research focused on developing secure and adaptive learning frameworks that respond to diverse learner needs. His current work, "Adaptive Federated Learning Algorithm for Privacy-Preserving Personalized Learning in E-Learning Systems with Dynamic User Interactions," explores innovative federated learning approaches that enable personalized educational experiences while protecting user privacy and ensuring data security. Through his research, he aims to advance intelligent, scalable, and privacy-aware e-learning ecosystems that support effective and adaptive learning outcomes.

Sherzod Zakirxodjaev is a faculty member at Tashkent State Medical University, Tashkent, Uzbekistan. He is actively engaged in teaching, research, and the application of advanced digital technologies to improve educational and healthcare learning environments. His academic interests include artificial intelligence, federated learning, privacy-preserving machine learning, educational data analytics, and personalized e-learning systems. He has contributed to interdisciplinary research focused on developing secure and adaptive learning frameworks that enhance learner engagement and educational outcomes. His current work, "Adaptive Federated Learning Algorithm for Privacy-Preserving Personalized Learning in E-Learning Systems with Dynamic User Interactions," investigates innovative federated learning approaches that enable personalized educational experiences while maintaining the privacy and security of user data. Through his research, he aims to advance intelligent, scalable, and privacy-aware e-learning ecosystems that effectively adapt to dynamic user interactions and diverse learner needs.

Komiljon Gulyamov is a Professor and Dean of the Faculty of Art History and Applied Arts at the National Institute of Fine Arts and Design named after Kamoliddin Bekhzod, Tashkent, Uzbekistan. He has extensive experience in higher education, academic leadership, and interdisciplinary research that bridges technology, creativity, and innovation. His academic interests include artificial intelligence, educational technologies, data privacy, personalized learning systems, and digital transformation in higher education. He has contributed to research initiatives focused on developing intelligent and secure learning environments that enhance learner engagement and educational outcomes. His current work, "Adaptive Federated Learning Algorithm for Privacy-Preserving Personalized Learning in E-Learning Systems with Dynamic User Interactions," explores advanced federated learning techniques that enable personalized educational experiences while ensuring the privacy and security of user data. Through his research, he aims to advance scalable, intelligent, and privacy-aware e-learning ecosystems that effectively adapt to the evolving needs of learners.

Khurshida Tillakhodjaeva is a faculty member at Tashkent State Technical University, Tashkent, Uzbekistan. She is actively engaged in teaching, research, and the application of advanced digital technologies to modern educational environments. Her academic interests include artificial intelligence, federated learning, privacy-preserving machine learning, educational data analytics, and personalized e-learning systems. She has contributed to interdisciplinary research focused on developing secure and adaptive learning frameworks that enhance learner engagement and educational effectiveness. Her current work, "Adaptive Federated Learning Algorithm for Privacy-Preserving Personalized Learning in E-Learning Systems with Dynamic User Interactions," explores innovative federated learning approaches that enable personalized educational experiences while ensuring the privacy and security of user data. Through her research, she aims to advance intelligent, scalable, and privacy-aware e-learning ecosystems that effectively respond to dynamic learner interactions and evolving educational needs.