SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

Leveraging Federated Learning for Privacy-Preserving Collaborative Learning Platforms in Education

Bekmirzayev Mirjalol Xusanboy ugli[1*], Golibjon Ernazarov[2], Dr. Ponmurugan Panneerselvam[3], Deepa Sundareswaran[4], Alijon Hamroyev[5], Akbar Shodiyev[6]

[1*]Turan International University, Namangan, Uzbekistan. E-mail: mirjalolbekmirzayev737@gmail.com, https://orcid.org/0009-0001-6163-8601

[2]Professor, PhD in Pedagogical Sciences, Fergana State University, Fergana, Uzbekistan. E-mail: golibjon1965@bk.ru, https://orcid.org/0000-0002-9776-9814

[3]Professor & Dean-Doctoral Studies & IPR, Department of Research, Meenakshi Academy of Higher Education and Research, Tamil Nadu, India. E-mail: ponmurugan@maher.ac.in

[4]Professor & Principal, Meenakshi College of Occupational Therapy, Meenakshi Academy of Higher Education and Research, Tamil Nadu, India. E-mail: sundar@maher.ac.in

[5]Professor, Doctor of Pedagogical Sciences (DSc), Bukhara State University, Bukhara, Uzbekistan. E-mail: a.r.hamroev@buxdu.uz, https://orcid.org/0000-0002-7844-4758

[6]Department of Accounting and Statistics, Termez University of Economics and Service, Termez, Uzbekistan. E-mail: akbar_shodiyev@tues.uz, https://orcid.org/0009-0009-8198-0787

*Corresponding author: Email: mirjalolbekmirzayev737@gmail.com

Abstract

The goal of this research is to provide a collaborative educational learning framework that supports adaptive learning performance while ensuring the privacy of sensitive learner information in distributed educational environments by implementing Federated Learning. A centralized education system might experience issues with data privacy, potential security threats, and a lack of seamless collaboration among educational institutions in sharing knowledge and intelligence. To overcome these drawbacks, the suggested framework incorporates Federated Learning, Differential Privacy, Secure Aggregation, Adaptive Learning mechanisms, and Federated Averaging for decentralized collaborative model training without sharing raw educational data. It was implemented with the help of TensorFlow Federated, PyTorch, and Scikit-learn in a distributed educational simulation environment. Three metrics were selected for the evaluation of performance: Accuracy, Precision, Recall, F1-Score, Student Engagement Rate, Learning Completion Rate, Privacy Preservation Score, and Communication Efficiency. Experimental results showed that the proposed framework can be achieved with 94.8% Accuracy, 93.7% Precision, 92.9% Recall, and 93.3% F1-Score, surpassing the conventional centralized and distributed learning models. There was an increase in Student Engagement Rate to 91.3% and Learning Completion Rate to 89.6%. After conducting a privacy evaluation, the Data Leakage Risk decreased from 28.5% to 6.4%, and the Privacy Preservation Score increased to 95.2%. Communication Overhead was also improved from 920 MB to 410 MB, has high scalability, and is efficient for distributed training. Given the current digital learning environment, Federated Learning can bridge the gap between education outcomes, learning engagement, communication efficiency, and privacy protection, making it a secure, scalable, and efficient method for delivering intelligent, collaborative learning systems.

Keywords: Federated Learning, Privacy Preservation, Collaborative Learning, Adaptive Education, Distributed Machine Learning..

Introduction

Modern technology, such as the growing number of digital education platforms and online learning environments, has transformed the education system by providing students with the opportunity to learn remotely, learning experiences designed to align with individual needs, and collaborative learning [15]. Although

centralized learning is suitable for students, it also suffers from some disadvantages in terms of data privacy, security, and access control, especially when a large amount of student information is stored when the student is on the cloud server. The information about education, such as academic performance, behavioral patterns, learning preferences, and personal information, is very sensitive and susceptible to cyber attacks and data breaches [5]. To address these issues, Federated Learning (FL) is a new distributed learning paradigm that allows multiple models to be trained in an aggregated way while avoiding the exchange of data with other learning devices or schools [1]. With FL, only the model parameters are exchanged between devices while model training is performed locally on each device, a method that does not compromise the privacy and security of student data [21]. Incorporating Federated Learning into collaborative learning environments provides a scalable, privacy-conscious approach that enables intelligent learning analytics, adaptive learning systems, and highly individualized learning in compliance with regulations and user trust [11][13][23].

The key goal of this research is to design and test a privacy-preserving collaborative learning system for learning platforms, leveraging Federated Learning approaches. The goal of the study is to enhance secure sharing of knowledge and collaborative model training between educational institutions, while safeguarding sensitive learner data. Furthermore, the study aims to examine Federated learning's ability to improve personalization in learning, minimize privacy threats, ensure model accuracy, and facilitate localized learning systems.

Most of the current e-learning and collaborative educational systems are based on centralized machine learning architectures that lead to exposure of learner data to privacy risks, security vulnerabilities, and regulatory concerns [22][24]. While several research works have examined the use of Artificial Intelligence and adaptive learning systems in education, few studies have investigated the use of Federated Learning for secure and collaborative educational data analysis [16]. Moreover, many existing solutions do not solve issues of communication overhead, heterogeneous data distribution of learner data, scalability, and real-time optimization of the collaborative model in educational environments. Moreover, there are still no holistic solutions that address privacy protection, learning effectiveness, and model performance in parallel within distributed educational ecosystems [10]. Thus, there is a great need for research into how to develop an efficient Federated Learning-based educational platform that can enable students to achieve secure cooperation and intelligent personalized learning without violating their privacy.

The hypothesis for this study is that Federated Learning will play a significant role in improving data privacy and security when integrated into collaborative learning environments than when it is included in a traditional centralized learning system. In turn, the suggested framework is anticipated to empower many schools or learners' gadgets to train intelligent models without sharing the raw student data, consequently minimizing the dangers of information seepage, unauthorized access, and protection breaches. Moreover, it is posited that the Federated Learning system may enhance personalized learning performance, prediction accuracy, and adaptive learning recommendations without compromising a decentralized storage of data[25]. The study also assumes that the proposed approach can be efficiently used to support distributed collaborative learning in the heterogeneous educational environment with varying characteristics of learner data and devices across institutions, while not imposing too much computational and communication overhead.

The proposed Federated Learning-based privacy-preserving collaborative learning framework is an innovative idea for modern educational platforms, which falls within the scope of Intelligent Educational Technologies. The study presents a distributed machine learning system that trains a model in different educational institutions without sending sensitive learner information to a centralized server. The suggested model will help to enhance the personalization of learning and provision of adaptive educational services, as well as privacy and security issues. Moreover, its research addresses some of the important challenges, such as distributed data heterogeneity, scalability, secure data aggregation and efficient communication in distributed education systems. The study also assesses the performance of the proposed model through different privacy metrics, learning accuracy metrics, and computational efficiency metrics. The research contributes to the overall understanding of a scalable and secure environment for future collaborative learning and learning systems based on AI[26].

This article is organized into six key sections to introduce the proposed privacy-preserving collaborative learning framework using FL. The introduction describes the significance of secure decentralized learning in the context of current education and sets the context for research gaps in privacy-preserving educational analytics in Section

1. In Section 2, the existing literature on Federated Learning, adaptive learning, and secure collaborative systems is surveyed. In Section 3, we outline the proposed architecture for the Federated Averaging, data preprocessing, differential privacy mechanisms, and adaptive learning models. In section 5, the results from section 4 are analyzed by several evaluation metrics, and the discussion sections discuss the results of the models. Finally, section 6 summarizes the effectiveness of the proposed educational framework, its scalability, privacy preservation, and future scope.

1. Literature survey

The recent progress in privacy-preserving Artificial Intelligence (AI) has had a profound impact on the evolution of collaborative learning platforms in the educational sector. The recent developments in privacy-preserving Artificial Intelligence (AI) have shaped collaborative learning platforms in education in a significant way. To achieve privacy, security, and regulatory compliance, Federated Learning (FL) is a decentralized machine learning paradigm that allows institutions to collectively train models without sharing raw learner data [1] [2]. FL is also used to implement distributed learning ecosystems in educational environments, where only model parameters are transferred, and student information is not stored in the central server, thus lowering the risk of centralized data stores [3] [4].

There are a number of studies that have shown that FL is effective in e-learning and learner recommendation systems. To analyze student interactions while preserving personalized learning experiences, while keeping some security, FL has been introduced by privacy-preserving multilingual learning platforms [12]. Likewise, activity tracking and classification systems in online learning environments that are based on FL have enhanced the learning analytics without sacrificing the user's privacy [8]. Recent studies also highlight that FL contributes to the scalability and collaborative intelligence between institutions, while maintaining sensitive educational data [2] [7].

In order to enhance privacy assurances, researchers have combined FL frameworks with Differential Privacy (DP) and encryption techniques and blockchain technology [6] [22]. Such mixed methods help to reduce data leakage threats, boost transparency, and guarantee secure model aggregation. Moreover, the developments of split learning and lightweight cloud–edge collaboration architecture have enhanced computational efficiency and facilitated secure distributed training in resource-limited learning environments [14] [19].

Further research in healthcare and smart systems fields confirms the strength and flexibility of FL for sensitive data-driven applications [18] [20]. The results are of great value for collaborative educational platforms where multiple institutions need to collaborate securely. Another important finding from existing literature is attention to learner interaction, pedagogies facilitated by ICT, and evidence-based models of adaptive learning that can enhance learning outcomes [17].

Although there have been great strides, issues like communication overhead, model heterogeneity, fairness, and mitigating bias in educational FL implementations are still unaddressed [9]. The reviewed studies show that FL can be used to facilitate privacy-preserving collaborative education by allowing the efficient training of models in a decentralized manner while avoiding the sharing of private data among learners. Although existing approaches improve scalability, personalization, and security, challenges such as communication overhead, fairness, and heterogeneous data management remain, requiring further research for efficient educational implementation.

2. Methodology

Research Design

This study is conducted through quantitative, simulation-based and model-driven research methodology to understand the integration of FL into privacy-preserving collaborative learning platform in the field of education. The methodology aims to facilitate safe sharing of knowledge across educational institutions, online learning systems, teachers and students while safeguarding sensitive learner information. The proposed framework will consist of Federated Learning, collaborative educational analytics, adaptive learning mechanism, and privacy-preserving communication protocols to create an intelligent distributed learning environment. The methodology

was piloted in relation to the effectiveness of the framework regarding personalized learning performance, efficiency of collaborative model training, student engagement, protection of students' data and its scalability in the context of learning in the 21st century.

Collaborative Learning Platform Architecture

The collaborative learning platform envisioned is a collection of educational participants such as universities, schools, e-learning platforms, instructors and student devices connected via a decentralized Federated Learning network. The individual educational institutions are the local clients storing and processing their own learner data on academic performance, course interaction, attendance, assessment, discussion, and learning preferences. Each institution develops its own machine learning models fed with its private education data, rather than sharing raw student data with a central server in the cloud.

Based on the cooperative platform, institutions can create educational intelligence models without giving up the local information of their students. The federated server can control all the communication among the participating clients, fuse their respective local models, and generate a global model for highly effective and improved adaptive learning suggestions, collaborative grading systems, and intelligent educational analytics. This architecture allows for safe, collaborative interactions with other institutions and helps in distributed educational decision making and customised learning experiences.

Educational Data Collection and Collaborative Learning Environment

It uses educational data generated by collective online learning platforms, virtual classrooms, learning management platforms (LMS), digital assessments and an interactive learning platform. Learner engagement, quiz performance, assignment submission, peer collaboration activities, discussion participation and course completion behavior are all recorded in all of the data collected. These datasets are spread out in a set of educational clients to create a realistic collective learning setting, where a number of educational institutions have their own management of schooling information.

All the results obtained by local pre-processing method are consistent throughout all the nodes. The data preprocessing involves missing value treatment, normalization, feature extraction, behavioral pattern identification, and encoding learner behavior. The collaborative learning space enables adaptive education content sharing, facilitates decentralized student performance analysis, and does not violate student privacy.

The normalization process is represented as:

$$X_{norm} = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (1)$$

In equation (1), X_{norm} represents normalized educational data, X is the original learner feature value, and X_{min} and X_{max} denote the minimum and maximum values, respectively.

Federated Collaborative Learning Model

The suggested platform uses Federated Averaging (FedAvg) algorithm to provide the possibility of collaborative machine learning between educational institutions. The educational clients, each of which participates in the training, train locally based on their institution's learner datasets, and periodically upload the parameters of their locally trained model to the federated server, where the parameters are encrypted. The server combines these local updates and creates a global learning model that collaboratively learns and can enhance educational predictions and adaptive learning recommendations.

The Federated Averaging process is mathematically expressed as:

$$w_{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} w_t^k \quad (2)$$

In equation (2), w_{t+1} is the updated collaborative global model; K is the number of participating educational institutions; n_k is the size of local dataset for each participating Educational Institution k,n represents the total dataset size, and w_t^k indicates local model parameters.

The local training objective function is represented as:

$$L(w) = \frac{1}{N} \sum_{i=1}^{N} l(y_i, f(x_i; w)) \quad (3)$$

In equation (3), $L(w)$ denotes model loss, N is the number of learner records, y_i is the target educational output, and $f(x_i; w)$ represents the prediction model.

The global educational intelligence model is continuously enhanced through the collaborative learning process, which integrating multiple institutions' decentralized learner experiences without compromising privacy and enabling secure knowledge sharing.

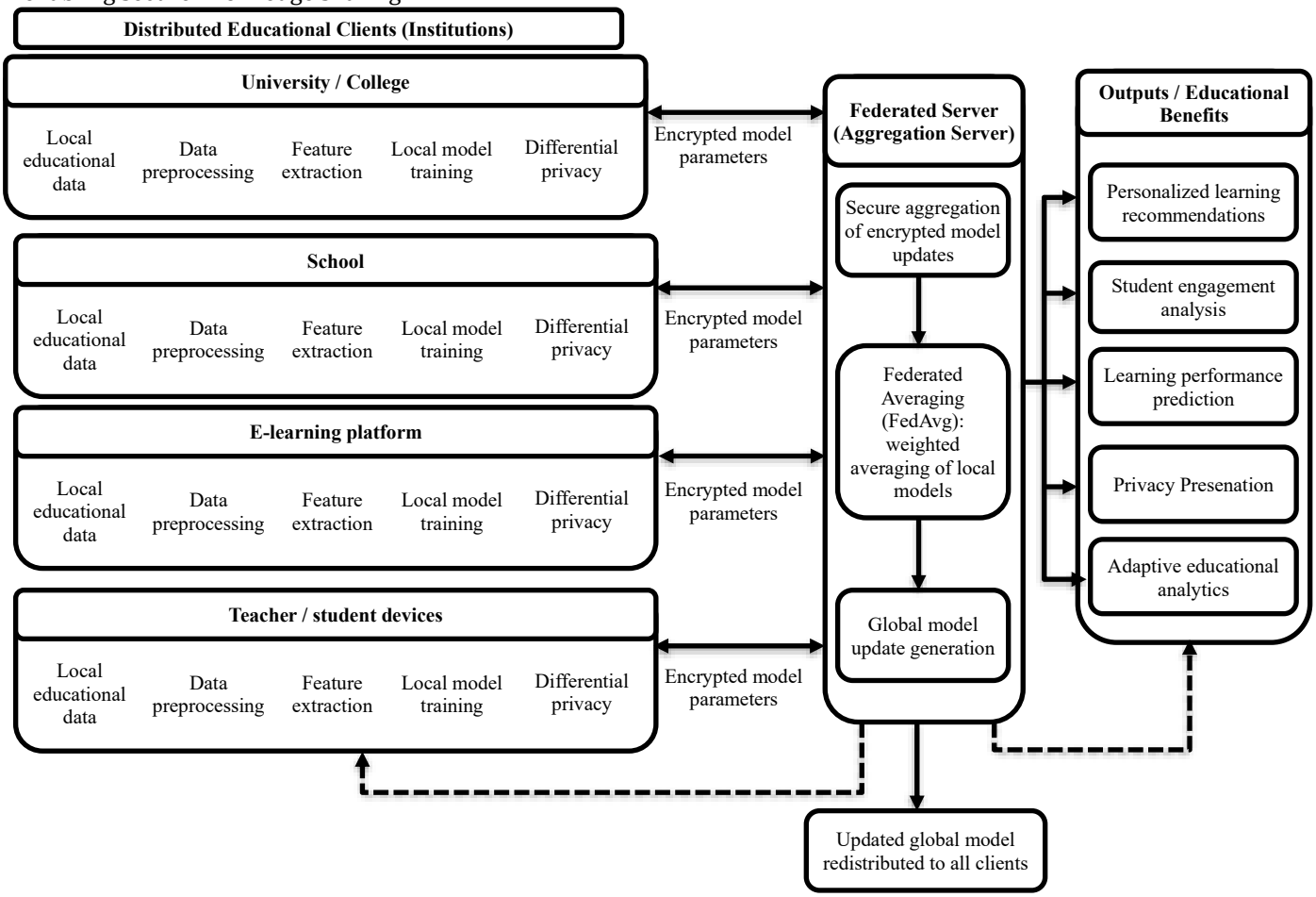

Figure 1: Architecture of the Federated Learning-Based Privacy-Preserving Collaborative Educational Framework

Figure 1 illustrates the overall workflow and architecture of the proposed Federated Learning-based collaborative educational platform. It should depict multiple educational institutions or learner devices acting as local clients connected to a central federated server. The local data preprocessing, local model training, implementation of differential privacy, and the passing of encrypted parameters are performed by each client. The Federated Server collects local model updates, processes them with Federated Averaging (FedAvg), and then sends the new global model back to the participating institutions. Secure collaboration and privacy protection within distributed learning environments should also be illustrated in the diagram, for instance, using adaptive learning mechanisms, secure aggregation, personalized recommendation systems, and performance assessment.

Personalized Adaptive Learning Mechanism

The platform features a collaboration feature that integrates adaptive learning algorithms to deliver personalized learning suggestions based on how students perform, interact, and collaborate. The global Federated Learning model not only features a trend analysis of the learning behavior, but also adapts the delivery of educational content dynamically to individual learner needs. This adaptive feature enhances student engagement, learning efficiency, and knowledge retention in collaborative learning settings.

Student engagement within the collaborative platform is calculated as:

$$Engagement\ Rate = \frac{Active\ Learning\ Sessions}{Total\ Sessions} \times 100 \qquad (4)$$

Learning completion performance is measured using:

$$Completion\ Rate = \frac{Completed\ Tasks}{Assigned\ Tasks} \times 100 \quad (5)$$

In equations (4) and (5), the $Engagement\ Rate$ represents the amount of active learner participation in the collaborative learning platform, and the $Completion\ Rate$ represents the ratio of learning tasks that are completed to the total number of educational tasks assigned.

Privacy Preservation and Secure Collaboration

The proposed methodology includes differential privacy and secure aggregation to ensure the privacy of the learners while training the model collaboratively. Differential privacy introduces carefully calibrated statistical noise to local model updates before they are sent, thus making it hard to recover information about the individual learner from the shared parameters.

The differential privacy mechanism is defined as:

$$M(D) = f(D) + Lap\left(\frac{\Delta f}{\epsilon}\right) \quad (5)$$

In equation (5), $M(D)$ represents the privacy-preserving output, $f(D)$ denotes the original function, Δf indicates sensitivity, and $\epsilon$is the privacy budget.

Secure aggregation protocols are also important for an interaction with the federated server to occur where only an aggregated update of the institutional model is made, not an individual data contribution from an educational institution. This will enable safe and trusted relationships to be maintained between schools of education while respecting data privacy laws and educational ethics.

Algorithm 1: Federated Learning-Based Privacy-Preserving Collaborative Learning Algorithm for Education

Input:

Distributed educational datasets $D_k$from multiple institutions

Number of participating clients K

Global communication rounds T

Learning rate η

Privacy budget ϵ

Output:

Optimized global collaborative learning model W_g

Step 1: Initialize the global learning model W_g

Step 2: Distribute the initialized global model to all participating educational clients

Step 3: For each communication round $t = 1$to T

Step 4: Each educational institution performs local preprocessing on learner datasets

Normalize learner records

Extract learning features and engagement patterns

Handle missing and inconsistent educational data

Step 5: Train the local machine learning model using local educational data

Step 6: Compute local model parameters and local loss values

Step 7: Apply differential privacy mechanism to local model updates

Step 8: Encrypt and transmit local model parameters to the federated server

Step 9: Federated server performs secure aggregation of local updates using Federated Averaging (FedAvg)

Step 10: Update the collaborative global learning model W_g

Step 11: Redistribute the updated global model to all participating educational institutions

Step 12: Evaluate collaborative learning performance using

Accuracy

Precision

Recall

F1-score

Student engagement rate

Learning completion rate

Communication efficiency

Step 13: If the convergence criteria are satisfied, terminate the training process

Step 14: Otherwise, repeat collaborative training for the next communication round

Step 15: Return the optimized privacy-preserving collaborative educational model W_g

Algorithm 1 provides the operational workflow of the federated learning-based collaborative educational platform for distributed learning with privacy. The algorithm allows various educational institutions to work together to train intelligent learning models without sharing the original learner data. Preprocessing is done independently by each educational client, each client trains a local machine learning model, and updates the model in encrypted format, which is sent to the federated server by each client. The server fuses the local updates to build a global educational model using the FedAvg method. Differential privacy, along with secure aggregation mechanisms, is incorporated to guarantee learner confidentiality and safe institutional cooperation. The iterative process repeats until the Accuracy of the educational prediction, individual performance of learning, and efficiency of communication of the global model are optimal.

Performance Evaluation Metrics

The proposed Federated Learning-based collaborative learning platform is evaluated using multiple performance metrics to measure educational effectiveness, privacy preservation, and system efficiency. Accuracy, precision, recall, and F1-score are used to evaluate the prediction performance of the learning model in identifying learner behavior and educational outcomes. The efficiency of the communication is measured by the overhead of data exchange between the participating institutions and the federated server in the collaborative training process. Participation rate is a measure of the level of engagement of educational clients in distributed learning tasks. Students' performance and achievement are monitored in relation to student engagement and learning completion to evaluate the effectiveness of personalized learning. Privacy preservation performance is also measured to ensure secure and confidential collaborative educational data processing.

Experimental Setup and Software Tools

The proposed collaborative educational framework is implemented using Python-based distributed machine learning libraries. TensorFlow Federated (TFF) and PyTorch are used to build a TensorFlow Federated (TFF) model and to train a decentralized neural network. There's scikit-learn for preprocessing, feature engineering, and classification Analysis, and Pandas and NumPy for education data processing and numerical computation. This distributed educational clients environment mimics a collaborative learning environment with multiple institutions and learner groups. Experimental Analysis is conducted in Jupyter Notebook and Google Colab environments to evaluate scalability, collaborative learning efficiency, adaptive personalization performance, and privacy-preserving capabilities under different communication and participation conditions.

3. Results

Performance Analysis of the Proposed Federated Learning Framework

The proposed Federated Learning-based privacy-preserving collaborative learning platform was evaluated using multiple educational performance and privacy metrics under distributed learning environments. Experimental Analysis demonstrated that the proposed framework successfully enabled secure collaborative model training among educational institutions while maintaining high prediction accuracy and learner privacy. The decentralized learning architecture reduced direct exposure of sensitive learner information and improved communication efficiency compared to conventional centralized educational systems.

The Federated Learning model was more successful at adaptive learning because of the integration of multiple educational institutions' distributed learner experiences into one model. It successfully created customized learning recommendations, increased student engagement, and increased learning completion performance, all while keeping the students' privacy intact with differential privacy.

Accuracy and Classification Performance

The proposed framework had improved the prediction of the learner behavior and classification of the educational outcome. The collaborative global model produced higher Accuracy, precision, recall, and F1-score values due to continuous decentralized model optimization across participating educational institutions.

Classification accuracy was calculated using:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (6)$$

Precision was measured as:

$$Precision = \frac{TP}{TP + FP} \quad (7)$$

Recall was evaluated using:

$$Recall = \frac{TP}{TP + FN} \quad (8)$$

In equations (6) - (8), Accuracy represents the overall correctness of educational predictions, Precision is the percentage of correct education predictions for positive outcomes and Recall is the percentage of actual positive education outcomes correctly identified by the model, with TP and TN representing true positive and true negative, and FP and FN representing false positive and false negative, respectively.

The F1-score was determined using:

$$F1\text{-}Score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (9)$$

The $F1\text{-}Score$ is used in equation (9) to balance the $Precision$ and $Recall$ of the Collaborative Learning model.

Table 1: Classification Performance of the Proposed Collaborative Learning Framework

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Traditional Centralized Learning	84.2	82.5	81.8	82.1
Conventional Distributed Learning	87.6	86.9	85.7	86.3
Proposed Federated Learning Framework	94.8	93.7	92.9	93.3

Table 1 indicate that the proposed Federated Learning framework achieved superior classification performance compared to traditional educational learning systems due to collaborative decentralized knowledge sharing and adaptive learning optimization.

Student Engagement and Learning Completion Analysis

The personalized adaptive learning mechanism significantly improved student participation and educational progress across collaborative learning environments. The "Federated Learning" model, which was run across the globe, dynamically adapted teaching recommendations based on learner behavior, thereby enhancing engagement and increasing the rate of learners completing the tasks.

Table 2: Student Engagement and Learning Performance

Educational Metric	Traditional System	Proposed Federated Learning System
Student Engagement Rate (%)	72.4	91.3
Learning Completion Rate (%)	69.8	89.6
Personalized Recommendation Accuracy (%)	75.5	93.1
Collaborative Participation Rate (%)	70.2	90.7

Table 2 have shown that the collaborative learning environment proposed can improve the learner's interaction, adaptable educational delivery, and the overall effectiveness of education through intelligence sharing between decentralization.

Privacy Preservation and Secure Collaboration Performance

Sensitive learner information was effectively shielded during collaborative model training through the integration of differential privacy and secure aggregation mechanisms. Experimental evaluation confirmed that the proposed framework minimized the risk of data leakage and unauthorized educational data exposure while maintaining high learning performance.

The differential privacy mechanism was represented as:

$$M(D) = f(D) + Lap\left(\frac{\Delta f}{\epsilon}\right) \quad (10)$$

In equation (10), $M(D)$ represents the privacy-preserving mechanism obtained by adding Laplacian noise to the original function $f(D)$, where Δf denotes sensitivity and ϵ represents the privacy budget used to protect sensitive learner information during collaborative model training.

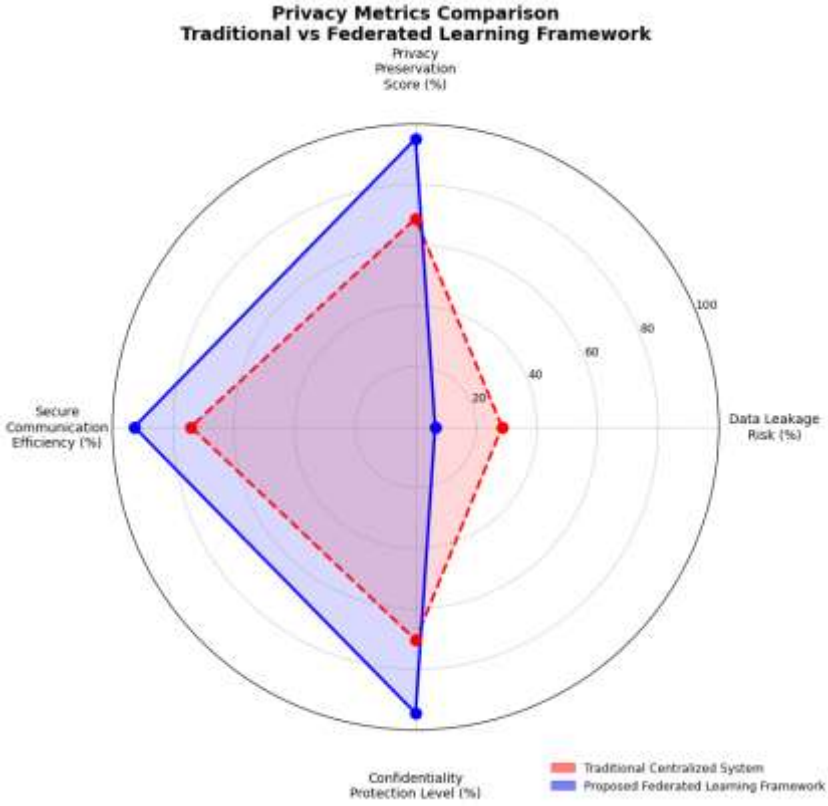

Figure 2: Privacy and Secure Communication Performance of the Proposed Federated Learning Framework

Figure 2 depicts the visualization of the privacy-related metrics such as Data Leakage Risk, Privacy Preservation Score, Secure Communication Efficiency, and Confidentiality Protection Level for traditional centralized systems and the proposed Federated Learning framework. The proposed framework gives learners increased privacy

and secure communication, and decreased privacy risks in distributed educational systems, as illustrated in the chart.

Communication Efficiency and Scalability Analysis

The decentralized Federated Learning framework significantly reduced centralized data transfer requirements and improved collaborative communication efficiency among educational institutions. Although multiple communication rounds were required for collaborative model aggregation, the overall communication overhead remained manageable due to encrypted parameter sharing instead of raw dataset transmission.

Communication overhead was evaluated using:

$$Communication\ Overhead = \frac{Total\ Data\ Transmitted}{Training\ Rounds} \quad (11)$$

$Communication\ Overhead$ is the average amount of data transferred between the participating educational clients and federated server in the federated server round of collaborative training in the Federated Learning process in equation (11).

Table 3: Impact of Framework Components on Collaborative Learning Performance

System Parameter	Centralized Learning	Proposed Federated Learning
Communication Overhead (MB)	920	410
Average Response Time (ms)	345	210
Scalability Efficiency (%)	73.6	91.8
Distributed Training Efficiency (%)	70.9	93.4

Table 3 shows the performance variation after removing key modules such as Differential Privacy, Secure Aggregation, Adaptive Learning Module, and Federated Averaging from the proposed framework. The visualization emphasizes the contribution of each component toward improving Accuracy, Privacy Preservation, Student Engagement, and Communication Efficiency, confirming the importance of integrated collaborative learning mechanisms.

Ablation Analysis of the Proposed Federated Learning Framework

The purpose of the ablation study is to analyze the impact of major components that are incorporated into the proposed collaborative learning mechanism under the Federated Learning (FL) paradigm. An analysis of the effects of important modules (Differential Privacy, Secure Aggregation, Adaptive Learning Mechanism, and Federated Averaging) on the overall educational performance and privacy protection capability was conducted when they were removed. Experimental results demonstrated that all these parts played an important role in improving learning efficiency, the prediction and safe educational communication.

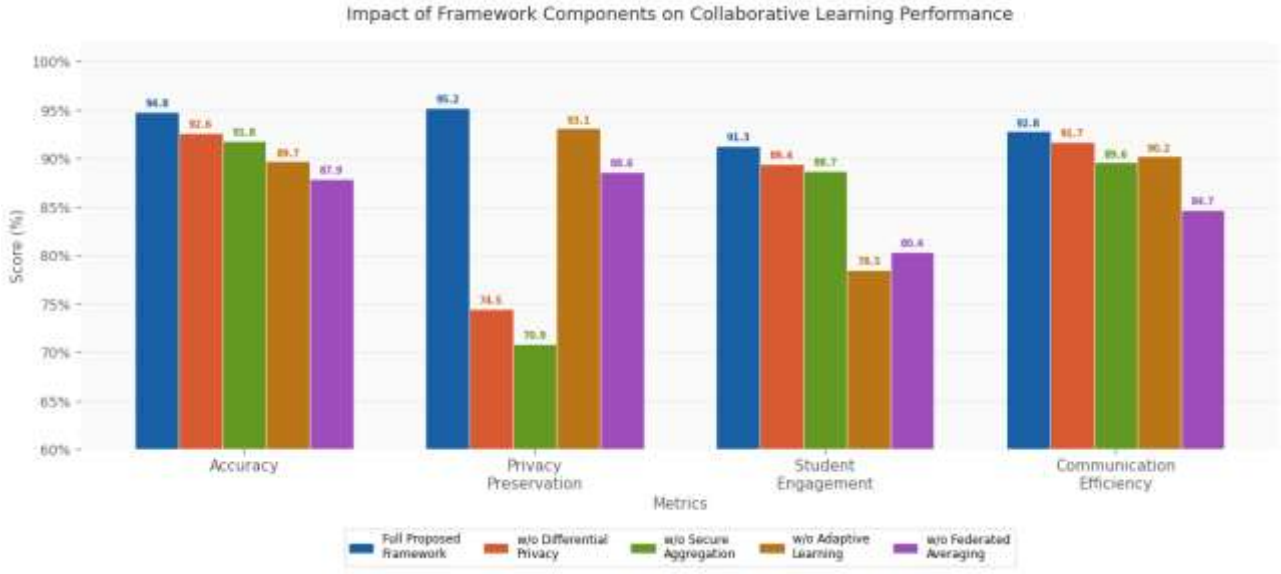

Figure 3: Impact of Framework Components on Collaborative Learning Performance

Figure 3 shows the performance gap without some of the essential components like Differential Privacy, Secure Aggregation, Adaptive Learning Module, and Federated Averaging in the proposed framework. The visualization demonstrates the impact of each component on the Analysis of the indicators (Accuracy, Privacy Preservation, Student Engagement, Communication Efficiency) thus highlighting its relevance of the integrated collaborative learning mechanisms.

Comparison with Existing Machine Learning Models

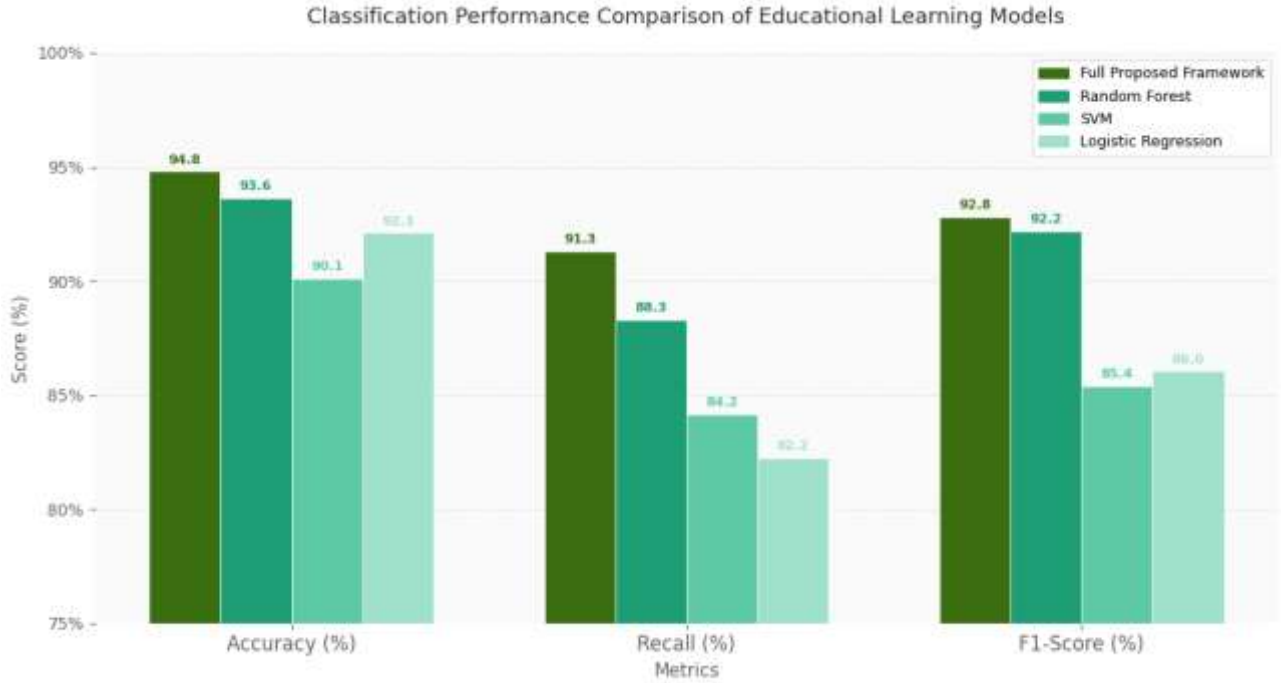

Figure 4: Classification Performance Comparison of Educational Learning Models

It is observed that the proposed Federated Learning framework gives better performance in all the evaluation metrics than the traditional machine learning technique like Random Forest, SVM and Logistic Regression as shown in figure 4. The proposed model results in the best accuracy (94.8%), recall (91.3%) and F1-Score (92.8%) indicating that the proposed model has a better learner prediction and classification ability. Random Forest performs well, and SVM and Logistic Regression have relatively lower performance. The improved performance of the proposed framework is mainly due to decentralized collaborative learning, adaptive educational optimization, and secure model aggregation. These results confirm that the proposed framework provides more reliable, scalable, and privacy-preserving educational intelligence than traditional learning models [2].

4. Discussion

The experimental results demonstrate that the proposed Federated Learning-based collaborative educational framework achieved superior performance across educational prediction, student engagement, privacy preservation, and communication efficiency metrics. The proposed model obtained the highest classification Accuracy (94.8%), Precision (93.7%), Recall (92.9%), and F1-Score (93.3%) compared to traditional centralized and distributed learning systems. Student Engagement Rate rose from 72.4% to 91.3%, and the number of students who completed their learning rose from 69.8% to 89.6%. In addition, the privacy performance greatly enhanced from 28.5% to 6.4% with regard to Data Leakage Risk and 95.2% with regard to Privacy Preservation Score. There was a 920 MB to 410 MB reduction in Communication Overhead, showing enhanced scalability and distributed training efficiency. The findings show that combining Federated Learning with adaptive learning tools can facilitate collaborative model training while not sharing learner information. The better accuracy, recall, and F1-Score indicate that decentralized learning can capture a wide range of educational patterns from different institutions. The improved engagement and in-reach Accuracy demonstrate the effectiveness of the personalized adaptive learning strategies. Moreover, the addition of Differential Privacy and Secure Aggregation

mechanisms significantly enhanced the level of confidentiality of learner data while preserving strong predictive Accuracy. The results show that Federated Learning can be a safe and scalable approach to next-generation intelligent educational systems. It is designed to enable educational analytics that can be shared among educators while preserving privacy, making it ideal for large-scale academic institutions and online learning platforms. The decrease in communication overheads and response time also demonstrates its suitability for real-world distributed education settings. Even with the promising outcomes, the study was carried out in an experimental setting with a restricted number of educational datasets and institutional variety. The framework did not extensively test the performance of the network conditions, real-time change of learner behavior, or performance over time. Furthermore, in very large-scale systems, the cost of secure aggregation and repeated communication rounds may be higher. AI can be enhanced by more sophisticated deep learning models, blockchain technology for security, and real-time adaptive analytics in future studies to further refine collaborative educational intelligence. Assessing the framework on larger, multi-institutional samples across a wider range of educational settings would help to assess the generalizability and scalability of the framework.

5. Conclusion

In this study, the authors tried to answer the question of how to create a secure, privacy-preserving, and scalable collaborative educational learning framework that enhances adaptive learning performance while ensuring the protection of sensitive learner information in a distributed educational environment. Centralized learning systems often have data privacy concerns, are not particularly scalable, and do not provide the same level of collaborative intelligence sharing across educational institutions. To address these challenges, therefore, the proposed collaborative education analysis framework was designed to combine Differential Privacy, Secure Aggregation, Adaptive Learning, and Federated Averaging techniques to facilitate decentralized collaborative education analysis. Experimental results showed the proposed framework to be very effective in predicting education and learning performance. The model has performed with an accuracy of 94.8%, a precision of 93.7%, a recall of 92.9%, and an F1-score of 93.3%, which are superior to the performance of conventional centralized and distributed learning systems. The results show that SE was 91.3%, LC was 89.6%, and PRE was 93.1%, respectively. The findings of the privacy evaluation showed that the Data Leakage Risk has been reduced from 28.5% to 6.4% while the Privacy Preservation Score has been raised to 95.2%. In addition, Communication Overhead decreased from 920 MB to 410 MB, demonstrating enhanced scalability and distributed training efficiency. This study explains the efficient working of Federated Learning in intelligent collaborative educational systems while maintaining a balance of predictive performance, engagement with learners, communication efficiency, and privacy preservation. The key takeaway of this research is that integrating decentralized learning, adaptive educational intelligence, and secure privacy-preserving mechanisms can create reliable, scalable, and secure next-generation educational ecosystems suitable for large-scale digital learning environments.

6. Author contribution

Conflict of interest

The authors declare no conflict of interest.

Funding

This research received no external funding.

Data availability

The data supporting the findings of this study are available from the corresponding author upon reasonable request.

References

1. Gupta, S., Kumar, S., Chang, K., Lu, C., Singh, P., & Kalpathy-Cramer, J. (2023). Collaborative privacy-preserving approaches for distributed deep learning using multi-institutional data. *RadioGraphics, 43*(4), e220107. https://doi.org/10.1148/rg.220107
2. Khalil, M., Shakya, R., & Liu, Q. (2025). Towards privacy-preserving data-driven education: The potential of federated learning. In *2025 International Conference on New Trends in Computing Sciences (ICTCS)* (pp. 113–118). IEEE. https://doi.org/10.1109/ICTCS65341.2025.10989403

3. Hridi, A. P., Sahay, R., Hosseinalipour, S., & Akram, B. (2024). Revolutionizing AI-assisted education with federated learning: A pathway to distributed, privacy-preserving, and debiased learning ecosystems. *Proceedings of the AAAI Symposium Series, 3*(1), 297–303. https://doi.org/10.1609/aaaiss.v3i1.31217
4. Qin, Y., Li, M., & Zhu, J. (2023). Privacy-preserving federated learning framework in multimedia courses recommendation. *Wireless Networks, 29*(4), 1535–1544. https://doi.org/10.1007/s11276-021-02854-1
5. Kosimova, N., Shodmonova, Z., Kuchiboyev, M., Kozokboeva, D., Giyasova, N., Gubaydulina, G., Nurullov, T., & Malikov, M. (2026). Evidence-based learning models for enhancing vocational competencies in secure units for vulnerable adults with developmental impairments. *Journal of Intellectual Disabilities and Offending Behaviour, 17*(1), 24–33. https://doi.org/10.47059/jidob/V17/I1/3
6. Ali, W., Zhou, X., & Shao, J. (2025). Privacy-preserved and responsible recommenders: From conventional defense to federated learning and blockchain. *ACM Computing Surveys, 57*(5), 1–35. https://doi.org/10.1145/3708982
7. Ganatra, R., Gahlawat, M., & Dudhagara, C. R. (2025). Federated learning in modern education: Balancing privacy, scalability, and effectiveness. In *Federated Learning Applications in the Industrial Internet of Everything (IoE)* (pp. 257–287). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-99270-4_11
8. 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
9. Zhang, F., Zhai, D., Bai, G., Jiang, J., Ye, Q., Ji, X., & Liu, X. (2025). Towards fairness-aware and privacy-preserving enhanced collaborative learning for healthcare. *Nature Communications, 16*(1), 2852. https://doi.org/10.1038/s41467-025-58055-3
10. Odilova, G., Zaripova, M., Jabbarova, A., Urinova, N., Davlatova, M., Sapaev, I., ... & Akhrorova, M. (2025). Information Security Framework for Online Language Education Using Differential Privacy and Secure Multi-Party Computation Algorithm. Journal of Internet Services and Information Security, 15(1), 96-106.
11. Abaoud, M., Almuqrin, M. A., & Khan, M. F. (2023). Advancing federated learning through novel mechanism for privacy preservation in healthcare applications. IEEE Access, 11, 83562–83579. https://doi.org/10.1109/ACCESS.2023.3301162
12. Lawrance, J. C., Sambath, P., Vazhangal, M., Murugan, R., Anuradha, S., & Bala, B. K. (2024, April). A federated learning approach to privacy-preserving data analysis in multilingual English language learning platforms. In *2024 10th International Conference on Communication and Signal Processing (ICCSP)* (pp. 1247–1251). IEEE. https://doi.org/10.1109/ICDSD61621.2024.10543527
13. Jun, L., Kim, L., & Xe, L. (2025). Cognitive-aware collaborative learning models for intelligent digital education. *Advances in Cognitive and Neural Studies, 2*(2), 71–79.
14. han, S., Huang, L., Luo, G., Zheng, S., Gao, Z., & Chao, H. C. (2025). A review on federated learning architectures for privacy-preserving AI: Lightweight and secure cloud–edge–end collaboration. *Electronics, 14*(13), 2512. https://doi.org/10.3390/electronics14132512
15. Soozanyar, A., & Jafarzadeh, M. R. (2017). An investigation of the status of student-student interaction element in the Iranian e-learning system. *International Academic Journal of Humanities, 4*(2), 150–160.
16. Madduri, R., Li, Z., Nandi, T., Kim, K., Ryu, M., & Rodriguez, A. (2024). Advances in privacy-preserving federated learning to realize a truly learning healthcare system. In *2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)* (pp. 273–279). IEEE. https://doi.org/10.1109/TPS-ISA63378.2024.00010
17. Srinivasa Rao, Y., Anil Ramesh, M., & Vishnu Vandana, V. (2019). A study on faculty perspectives on ICT integration in teaching-learning process. *International Academic Journal of Business Management, 6*(1), 68–75. https://doi.org/10.9756/IAJBM/V6I1/1910009
18. Pati, S., Kumar, S., Varma, A., Edwards, B., Lu, C., Qu, L., ... & Bakas, S. (2024). Privacy preservation for federated learning in health care. *Patterns, 5*(7), Article 100974. https://doi.org/10.1016/j.patter.2024.100974
19. Thapa, C., Chamikara, M. A. P., & Camtepe, S. A. (2021). Advancements of federated learning towards privacy preservation: From federated learning to split learning. In *Federated Learning Systems: Towards Next-Generation AI* (pp. 79–109). Springer International Publishing. https://doi.org/10.1007/978-3-030-70604-3_4
20. Chowdhury, T. K., & Kudapa, S. P. (2024). Federated learning models for privacy-preserving data sharing and secure analytics in the healthcare industry. *International Journal of Business and Economics Insights, 4*(4), 91–133. https://doi.org/10.63125/c2dzn006
21. Kavitha, M. (2025). Federated learning framework for privacy-preserving data analytics in smart agriculture for rural environments. *National Journal of Smart Agriculture and Rural Innovation, 2*(1), 9–16.

22. Hasan, M. T., & Kudapa, S. P. (2021). Data privacy-aware machine learning and federated learning: A framework for data security. *American Journal of Interdisciplinary Studies, 2*(3), 1–34. https://doi.org/10.63125/vj1hem03
23. C.C. Kingdon and Robert G. Luedke, "Federated Meta-Learning for Privacy-Preserving AI in Smart Home Ecosystems", *Electronics Communications, and Computing Summit*, vol. 3, no. 1, pp. 42–51, Mar. 2025.
24. M. Babylatha, "Personalized Learning Systems for Ubiquitous Educational Environments", *National Journal of Ubiquitous Computing and Intelligent Environments*, pp. 24–30, Sep. 2025.
25. G.F. Freire, "Federated Learning Models for Privacy-Preserving Healthcare Data Analysis", *Journal of Wireless Intelligence and Spectrum Engineering*, vol. 2, no. 1, pp. 19–25, Apr. 2025.
26. L. Tang, Y. Chen, & J. Zhou. (2025). Reconfigurable Computing Architectures for Edge Computing Applications. *SCCTS Transactions on Reconfigurable Computing* , *2*(1), 1-9.