Musik in bayern

ISSN: 0937-583x Volume 88, Issue 10 (Nov -2023)
https://musikinbayern.com

DOI https://doi.org/10.15463/gfbm-mib-2023-*254*

HYBRID FEDERATED LEARNING BASED PRIVACY-PRESERVING ON-SCREEN ACTIVITY TRACKING AND CLASSIFICATION IN E-LEARNING

N.Vaishnavi[1] *, Dr. A.Devi*[2]

[1]*Ph.d Scholar, Department of Computer Science, Dr. SNS Rajalakshmi College of Arts and Science, India.*

[2]*Associate Professor, Department of Computer Applications, Dr. SNS Rajalakshmi College of Arts and Science, India.*

E-Mail:Vaishnavi23sep@gmail.com

To Cite this Article

N.Vaishnavi*, *Dr. A.Devi,"* HYBRID FEDERATED LEARNING BASED PRIVACY-PRESERVING ON-SCREEN ACTIVITY TRACKING AND CLASSIFICATION IN E-LEARNING *"Musik In Bayern, Vol. 88, Issue 10, Nov 2023, pp225-254

Article Info

Received: 24-10-2023 Revised: 04-11-2023 Accepted: 14-11-2023 Published: 24-11-2023

Abstract: The internet is widely available as the fourth industrial revolution progresses. Digital gadgets are now necessary tools for both business and educational settings. Online education has grown at an exponential rate in recent times, removing obstacles based on geography and providing an adaptable learning setting. The utilization of e-learning, a contemporary teaching approach that makes utilization of electronic devices like computers, smartphones, and the internet, has grown significantly in popularity in the last several years. Although it might reach all parts of the globe, it presents a chance for resource and time waste. Students virtually constantly utilize the same device for both amusement and research. With social networks only a click away, students find it extremely challenging to utilize digital gadgets to research and to avoid wasting time on the platform. Given that online learning will become more and more common in the future, this is a really important issue. Despite this, there is a dearth of studies on identifying students' on-screen behavior, and none that aware of takes privacy protection into account. Thus, utilizing Federated Learning with Particle Swarm Optimization Algorithm (FLPSO) for protecting user privacy, a privacy-preserving structure is developed for this study to determine whether students utilize their computer time or squandering it. Numerous pre-trained algorithms are employed to categorize students into groups based on a dataset of over 4000 screenshots of their various activities; the suggested approach performs superior when considering of precision, accuracy, recall, loss, F1-score, and confusion matrix.

Keywords: E-learning, activity tracking**,** privacy-preserving and Federated Learning with Particle Swarm Optimization Algorithm (FLPSO).

1. INTRODUCTION

A growing number of scenes utilize computers as auxiliary structures, and some of these systems depend on record devices such cameras [1,2]. With so many cameras around, they are entitled to and can record a lot of data, most of which is personal. In the conventional teaching approach, the only way to receive feedback on the outcomes of teachers' lessons is through the school-organized centralized assessment. Yet this approach is time-consuming (taking anywhere from one month to six months), and students will suffer greatly if results are not received in a timely manner. Thus, to support instructors in carrying out their instructional duties, a comprehensive set of aid systems must be established [3,4]. Utilizing the classroom monitoring technology, it provides real-time evaluation and feedback on the learning state of the pupils. However, the system assesses the productivity of teachers. To enable to create a viable approach, an important amount of course videos must be gathered as training data. Teaching aids can be implemented in the classroom utilizing the teaching aid system, which was built utilizing a lot of data from several classes. But gathering and keeping these data which include student faces is prohibited [5]. Individuals requires permission before having their face data saved or shared in order to defend their right to privacy. Large amounts of labeled data are crucial for developing systems with high recognition rates, making labeling data of the most significant aspects of data collecting. This implies that take part in model training without being watched, saved, or communicated, the student's facial data must be labeled and employed as training data. Therefore, maintaining personal anonymity while building a framework without sacrificing accuracy is crucial. Cryptographic solutions protect the data from intruders trying to access it without authorization. Problems about privacy breaches arise, though, because they are not instantly applicable to stop authorized agents from abusing data without authorization [6]. Substantial losses will result from an attack on the server or a leak of the back-end data. When gathering videos, some scholars purposefully lower the recognition resolution in an attempt to study behavior through hazy footage. This has the benefit of allowing behavior recognition to be done while maintaining (facial) privacy protection [7]. It is clear that this approach has drawbacks. First, the video is blurry, which makes the upcoming recognition task more challenging; second, the inability to utilize the expression data adds to the recognition difficulties. Some studies avoid identifying specific people by employing behavioral evaluations of groups [8] or employing volunteers to train algorithms. Instead, computers handle the majority of data processing and modeling on their own without the need for human input in order to protect privacy. In this manner, privacy can be preserved while training the model with more realistic personal behavior data. Nevertheless, this approach needs a lot of data and label assistance, and sometimes it's hard to get a lot of data samples.

The worldwide e-learning market is anticipated to reach $325 billion by 2025, with the expansion of online learning set to soar in the following years. Ensuring student participation in online education presents particular difficulties. The risk of wasting time and resources unnecessarily is the difficulties with online learning [9]. It is challenging for students to stay focused on academic work when they frequently utilize the same gadget for both enjoyment and learning because social media and other distractions are just a click away. Students frequently access social media while utilizing a digital gadget for academic purposes, even unknowingly. As an outcome, rather of devoting them to their research, they conclude wasting significant time. Social media usage was shown to have a detrimental effect on educational achievement by S. Khan et al. [10], especially for those that utilized it more frequently. This result is in line with studies conducted by Geot [11]. u. et al. collect data from a sample of 379 students at four universities in the Khyber Pakhtunkhwa region utilizing a cross-sectional survey design [12]. According to the findings, most of students thought social media had a detrimental effect on their education. Additionally, the research discovered a positive correlation between social media usage and the belief that it has a detrimental effect on academic achievement. Many analyses demonstrate the substantial rise in online learning, which has been fueled by elements including technological advancements, rising internet usage, and a global trend toward distant learning [13]. Prioritizing the standard of the learning experience while establishing that students maximize the most of their time rather than becoming sidetracked by social media while participating in online educational tasks are becoming more and more crucial as the e-learning ecosystem grows. Social media site blockers are not always the best option, despite the fact that they are frequently suggested as a strategy to reduce distractions and improve pupil concentration in classroom settings. The main reason for this is that social media site blockers mainly work at the browser or device level, depending on the students' self-control to enable and enforce them. When confronted with the temptation to utilize social media systems, students may figure out ways past the blockers or disable them altogether. It's critical to recognize the dual functions that social media platforms like YouTube can play in terms of teaching and entertaining. Thus, it might not be logical or advantageous to use a basic site blocking strategy that is only focused on URLs [14]. Therefore, instead of depending on URL-based site tracking, suggested a successful method that entails examining the content that is really shown on the screen. It is imperative to recognize that applying conventional machine learning algorithms to computer screen evaluation presents legitimate privacy issues because the procedure requires uploading raw data to a central server. Provide a federated learning-based system for the identification and categorization of private computer activity in an e-learning environment to overcome these difficulties. The suggested structures, which combines the benefits of transfer learning with federated learning to offer a practical and private-preserving solution, is presented in this study along with its creation, execution, and assessment [15]. This method protects end user privacy by dispersing the learning function over numerous devices and guaranteeing that sensitive data stays local. Transfer learning makes it possible to adapt already learned models to various learning settings, which lowers the costs associated with computing and training time. In addition, the study addresses the the structure's possible uses, practical issues, and ethical implications in the larger context of e-learning. The idea is to utilize these studies to further the development of an on-screen activity detection method that is more reliable, secure, and sensitive to privacy.

Thus, FLPSO is employed as a method to secure user privacy while proposing a privacy-preserving framework to determine whether students are employing or squandering their computer time.

2. RELATED WORK

Here, review the some of the recent technique for the prediction of student performance with privacy preserving in e-learning environment.

Anwar et al [16] presented a privacy-preserving RM structure that permits the safe transfer of reputation. As an example, successfully pilot the RM system in an e-learning community and implement the reputation transfer protocol in a prototype way. A safe and effective anonymous authentication system was created by Jegadeesan et al. [17] specifically to prevent naughty students and subject matter experts from accessing OES. The suggested plan gives OES users the fundamental security need of user privacy up until they behave appropriately. The mechanism exposes the privacy of users who misbehave if there is any possibility of dispute. In comparison to other current systems, the security and performance assessment component of the system assures that it consumes very little data processing and transmission delay, thus providing an efficient platform for promoting sustainable learning utilizing resource-limited IoT devices. An online educational system that offers suggestions for learners to enhance their learning was created by Bagunaid et al. [18].A RNN is employed to calculate individual scores according to exam results and student participation. After that, a DBSCAN with Mahalanobis distance clustering is put into practice to put students into groups according to the score values they received. The created clusters are verified employing the estimation of entropy and purity. Utilizing the score-based cluster, a TMR technique is employed to forecast outcomes for students. Learners are separated into two categories when it comes to predicting their grades: average and poor. The former is further broken into below- and above-average students, while the latter is further separated into poor and very poor pupils. The objective of this classification is to offer helpful learning suggestions. The R-SARSA method, a suggested method, is included for assessment. It was mandatory for the students to complete their assignments in accordance with the suggested methods. Better results are obtained by this e-learning suggestion technique regarding false-positives, true-positives, recall, precision, and accuracy.

Nagarathinam et al [19] developed a recommendation system Similar to how they applied to the formless structure, the affiliation standard may be relevant for large E-Learning datasets. The applications of the affiliating rule after obtaining under-straight data from LMS for a large amount of time were investigated in this test. Analyzing a few affiliation rule computations leads to the discovery of intriguing quality metrics and other relevant understudy inclinations. A few hypothetical rule introductions and the corresponding results they apply will be demonstrated in terms of phrase reasonableness in online learning environments.

Rodriguez-Garcia et al [20] proposed a data mashup technique that can combine and *k*-anonymize data sets in cloud-based learning settings without compromising the data's analytical value. The protocol's deployment is built on linked data, which allows the data sets utilized in the mashups to be semantically characterized and combined with pertinent educational data sources. The approach still returns *k*-anonymized data sets with the necessary data to facilitate activities involving statistical evaluation and general data exploration. The results of the logical and experimental tests demonstrate that the suggested methodology keeps private data about individuals from being re-identified. Samad et al [21] presented the improvement of the PPDM framework for forecasting students' success on learning results in improved data mining accuracy and data privacy protection. This PPDM integrates homomorphic encryption with k-anonymization, two privacy-preserving techniques. In contrast, highest accuracy is found by comparing classification methods employed for data mining, such as Random Forest, SVM, and NB. It is anticipated that the suggested PPDM approach will provide higher privacy preservation and improved prediction accuracy for students' achievements on educational goals.

Ashwin et al [22] developed an approach for a face de-identification system which employs an input facial image for generating a new face while preserving the emotion and non-biometric facial features of a target face. Select the proxy set face that matches the target face with regard to of posture and facial expression. The proxy set includes a large number of synthetic faces created by StyleGAN. The chosen face from this collection is completely anonymous because the faces in the proxy settings were created artificially. generated a dataset with ten students to evaluate the approach. The created face maintained emotional qualities with a de-identified face, according to the findings of StyleGAN's performance evaluation for common metrics like gender and emotion.To address this problem, Xu et al. [23] developed a recommendation system for privacy-preserving educational systems that utilizes the different levels of privacy. Particularly a directed acyclic graph approach is employed to categorize each student based on their talents in a class. The technique known as differing privacy, which allows a facility to extract valuable data from databases holding people's personal information without disclosing sensitive identifying about any individual, is employed in the approach. Users can get personalized real-time data while maintaining their privacy according to a smart system of suggestions built on collaborative filtering. Tajanpure et al [24] suggested superior mining accuracy obtained by C-PPA, which converts the input into lower dimensions while maintaining anonymity. Several privacy-preserving criteria, including accuracy, precision, recall, and F1-measure, are employed to assess the suggested approach. When comparing findings with and without C-PPA, simulations conducted indicate that the average increment in accuracy of C-PPA for CNN classifier is 14.15. Overlap-add For parallel processing utilizing overlap-add convolution, C-PPA is suggested. For CNN, the average accuracy increment is displayed as 12.49. The statistics demonstrate the method's advantages in terms of performance, data value, and privacy protection. The method lowers the dimensions of the data, which lowers the cost of Internet connectivity. Mistry et al [25] presented a privacy-preserving structure to determine whether students are spending or wasting their computer time while federated learning protects user privacy. Various trained models are employed to categorize students into groups based on a dataset of over 4000 screenshots of their various activities; the suggested FedInceptionV3 model obtains an innovative test accuracy of 99.75%.

3. PROPOSED METHODOLOGY

In a typical situation, people can wish to work or play on their laptops. This will be detectable in a way that protects privacy according to the suggested approach. The figure 1 workflow diagram provides a step-by-step explanation of the suggested architecture.

- A user-friendly privacy-preserving structure that can identify students' productivity in online classes is provided, constituting the research's entirety.
- Guided Stochastic Gradient Descent (GSGD) Algorithm to optimize the specified learning rate
- Created Hybrid Federated Learning Architecture to utilize six well-known deep learning techniques for the classification of on-screen activities.
- Deep learning techniques plays an important role in classification and prediction of student performance, thus improving student performance prediction system.
- Six individual models are thoroughly analyzed in terms of efficiency, with measures such as precision, accuracy, recall, loss, F1-score, and confusion matrix supplied.

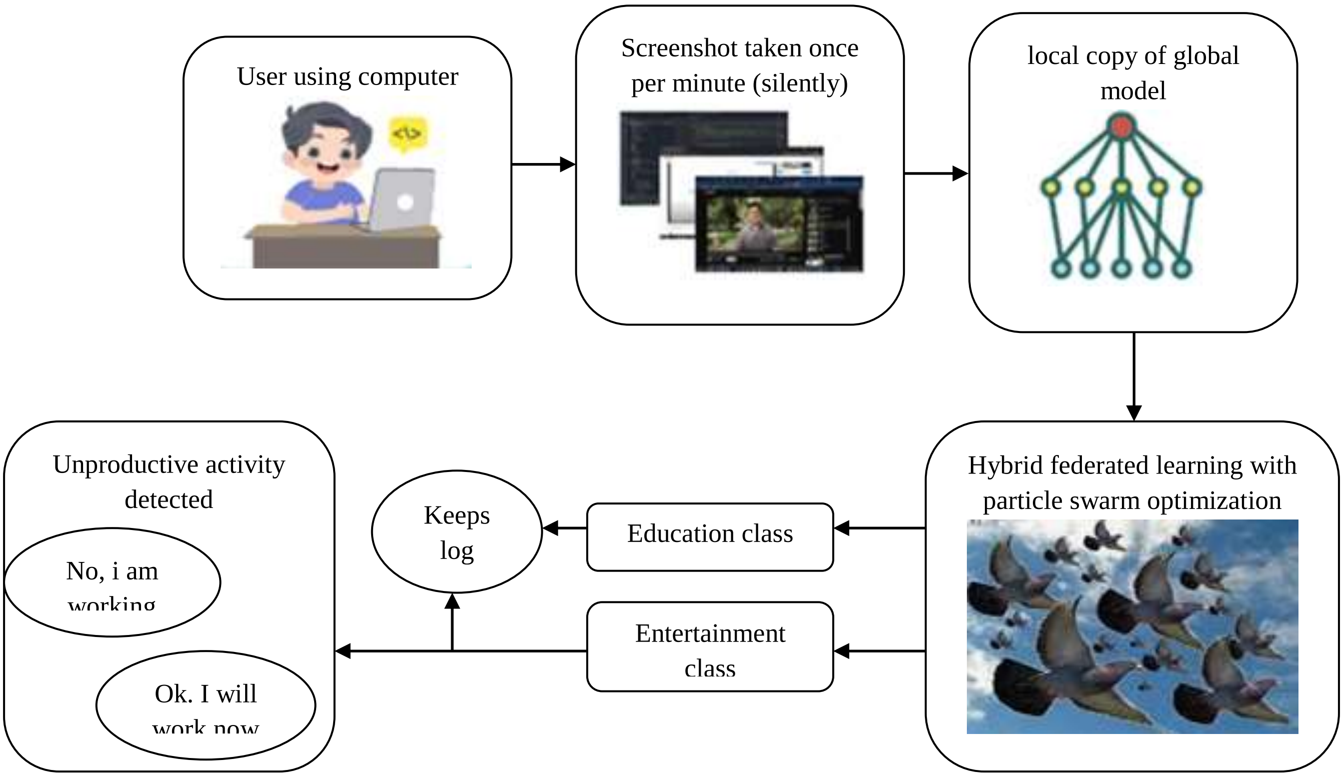
User using computer
Screenshot taken once per minute (silently)
local copy of global model
Hybrid federated learning with particle swarm optimization
Education class
Entertainment class
Keeps log
Unproductive activity detected
No, i am working
Ok. I will work now

Figure 1. the overall process of the proposed methodology

3.1. Framework Explanation

Step 1: The system will secretly capture a full screen snapshot once every minute as soon as its services are launched. TABLE 3. Activity detection log format.

Step 2: The screenshot will then be examined by the local model and categorized as either belonging to the entertainment or education classes.

If the screenshot is related to education classes, the application remains silent and classifies the log as beneficial. Table 3 displays the various formats in which the logs are maintained.

The user will receive notification via a pop-up window labeled "Unproductive Activity Detected" if two consecutive screenshots are from the entertainment class. This pop-up offers the following options, each of which has corresponding implications.

∗ No, I Am Working: Selecting this option marks the log as effective, modifies the model's settings, and considers the prediction as a failure.

∗ Okay, I Will Work Now: Selecting this option marks the log as entertaining and considers the prediction as successful, maintaining the model's parameters.

∗ X: The service will cease when the X option is clicked, and no logs will be visible in the final snapshot.

After the log is registered, all screenshots are completely deleted from the local device, minimizing the possible strain on the system resources. It was decided to set the time duration to identify inefficient action to one minute to reduce the possibility of diversions generated by the system. This method was selected because it was thought that a short burst of ineffective work would not have a major effect on the user's overall output. The user might consider it counterintuitive and possibly discouraged from employing a system that constantly produces notifications for each instance of inefficient activity. It is feasible for entertaining YouTube adverts to show up when people are watching instructional YouTube video. Under such circumstances, the event can be categorized by the system as an ineffective activity. In order to solve this problem, the machine is set up to take a silent screenshot once every minute and notify the user only if two consecutive screenshots show behavior that is not productive. The user is unlikely to receive a false alarm because the interesting YouTube ad would have probably skipped or terminated within a minute, avoiding the needless alarms from being generated.

By employing this technique, the system hopes to minimize user disturbances while maintaining its efficacy in recognizing useless activity. Therefore, the system is able to determine whether or not a user is spending their time on their computer in an intuitive way.

3.2. Privacy Preservation with Federated Learning

Federated learning protects user privacy within the system. In a conventional ML structure, if the system had been put on a single, central server, it would have required screenshots to be uploaded to a central cloud in order for it to be trained. This exposes the user's privacy and provides a tremendous opportunity for a security attack. Federated learning offers privacy protection by allowing ML algorithms to be developed on decentralized data sources instead of necessitating the centralization of data in one place. Federated learning keeps the data on the specific devices or servers that produce it, and it trains the model cooperatively on each of these decentralized data sources. Only updated model weights are communicated back and forth among the devices and the central server; the framework itself is not shared with any specific devices or servers.

This implies that specific data sources don't require to be provided with the central server, and the framework itself is not required to be aware of the particular data points it is learning from. Federated learning consequently renders privacy-preserving ML possible since the data is safe and private on the devices or servers that provide it, and the algorithm can still be trained successfully without jeopardizing the data's privacy.

Data is first accessed at the input layer in the structure that is suggested for the decentralized training of an algorithm. For assurance that every image is same, the photographs are scaled to a predefined shape with predetermined pixel values because the current setup only permits identical data. After that, clients are given random access to the dataset. A global training loop is established in which each client receives a copy of the global structure, and the local model weight is adjusted to match the weight of the global framework. Local data is utilized to train, test, and validate the local algorithm. Following the collection of the local weights, the global algorithm's new weight is determined by averaging all the weights, and the local clients receive their updated weight. Hence, the number of epochs determines how many times the globaltraining loop is performed.The complete procedure of this suggested method for training the framework decentralized and guaranteeing user privacy protection is shown in Figure 2. The pseudo-code presented in Algorithm 1 explains how Federated Transfer learning was included into this system.

Algorithm 1 Federated Learning Algorithm with FedAvg

```
Require: Pre-trained model $M_0$
Require: Client dataset $D = \{D_1, D_{2,......,}D_n\}$
Require: Categorical cross-entropy loss function L
Require: stochastic Gradient Descent (SGD) optimizer with learning rate Ƞ
Require: Number of communication rounds T
Require: Number of local epochs E
Require: Local mini-batch size B
Ensure: Global Model $M_{global}$
$M_{global} \leftarrow M_0$
for t=1 to T do
    for each client i=1, …., n in parallel do
        $M_i \leftarrow M_{global}$
        for e= 1to E do
            Shuffle $D_i$
            for each mini-batch $(x_{1,} y_1)$,…, $(x_B,y_B)$ in $D_i$ do
                $g \leftarrow \frac{1}{B}\sum_{j=1}^{B} \nabla L\big(M_i(x_j), y_j\big)$
                update $M_i$ using SGD: $M_i \leftarrow M_i - Ƞg$
            end for
        end for
    end for
    aggregate models using FedAvh: $M_{global} \leftarrow \frac{1}{n}\sum_{i=1}^{n} M_i^t$
end for
```

1) Algorithm Explanation

The federated learning algorithm define leveragesa pre-trained model *M*0, a collection of client datasets D, and categorical cross-entropy loss function *L*. The optimization achieved by stochastic gradient descent (SGD) with aspecified learning rate η. For a predetermined number of communication rounds (*T*), the system operates. Clients use their own datasets to update their local models for a given number of local epochs (*E*) and local mini-batch size (*B*) throughout each communication round. This is a detailed description of the method.

1) Initialize the global model *Mglobal*with a pre-trainedmodel *M*0.

2) To facilitate interaction among the server and the clients, carried out a predetermined number of communication rounds, *T*.

3) Iterate across each client *i* in parallel for every communication round *t*.

4) Associate each client's local model *Mi* to the current global model *Mglobal*.

5) Update each client's local model utilizing its corresponding dataset *Di* by carrying out a predetermined number of local epochs *E*.

6) To guarantee that the mini-batch selection process is random, shuffle the client's dataset *Di*.

7) Calculate the average gradient g of the categorical cross-entropy loss function *L* for each mini-batch in *Di* by comparing the predictions of the model *Mi(xj)* with the corresponding labels *yj*.

8) Utilizing the obtained gradient g and a learning rate η , update the local model *Mi* utilizing SGD.

9) Steps 4–8 should be repeated for the designated number of localepochs *E* so that the client may utilize its own dataset to optimize its local model.

10) Employ Federated Averaging (FedAvg) to aggregate the models of all clients when they have finished their local updates.

11) Use FedAvg by calculating the weighted average of the model parameters for each customer, granting greater datasets to clients.

12) Update the global system *Mglobal* with the aggregated system attained from the FedAvg step.

13) Repeat steps 3-12 for the specified number of communicationrounds *T* to progressively improve the globalmodel.

Following the federated learning process, the final global model, or Mglobal, is the result of collaboratively extracting knowledge from the datasets of all participating clients. Utilizing this method allows the global algorithm to maximize the use of the wide range of information that is present in each client's dataset, which makes the algorithm more robust and complete. This collaborative approach is significant because it protects the fundamental tenet of data privacy by guaranteeing that raw data stays private and isn't shared with the central server or other clients. Thus, the final global structure produced by federated learning is a compelling and appealing solution for distributed ML settings since it provides improved performance together with a strong commitment to maintaining data privacy.

Federated learning addresses important challenges including data privacy, data security, data access rights, and getting to heterogeneous data by allowing different players to develop a single, strong ML system without sharing data. Adversarial attacks over the privacy of data and the reliability of the learning model pose a challenge to federated learning as ML employs a distributed strategy to address local and global learning. The issue is solved by the integration of enhanced particle swarm optimization (EPSO).

3.3. Enhanced Particle Swarm Optimization (EPSO)

To get the optimal answer, Particle Swarm Optimization (PSO) employs a large number of particles that move around in the search space as a swarm. Every particle is viewed as a point in a D-dimensional space, and it modifies its "flying" in accordance with both its own and other particles' flying experiences [26]. To identify the best answer, the particles travel in D-dimensional space at a specific speed.

The particle i velocity $V_i = (v_{i1}, v_{i2}, \ldots, v_{iD})$, the particle i location is $(x, x_{i2}, \ldots, x_{iD})$,, the particle i optimal location is$p_g = (p_{g1}, p_{g2}, \ldots, p_{gD})$, it is also termed as p_{best}.

Another name for the global optimum position of all particles is g_{best}, and it is expressed as $p_g = (p_{g1}, p_{g2}, \ldots, p_{gD})$. To determine the fitness value, each particle in the group has a fitness function. The velocity update equation for dimension d in standard PSO is displayed in equations (1) and (2):

$$v_{id} = w \times v_{id} + c_1 \times rand() \times (p_{id} - x_{id}) + c_2 \times Rand() \times (p_{gd} - x_{id}) \quad (1)$$

$$(X_{id} = x_{id} + v_{id}) \quad (2)$$

PSO parameters contains: w (inertia weight), Q (Population Quantity), C1and C2 (acceleration constants), G_{max} (the maximum number of iterations), v_{max}(the maximum velocity), rand ( ) and Rand ( ) are random functions with values in [0,1]. The value of C1and C2usually takes constant 2. The figure 2. shows the process of EPSO.

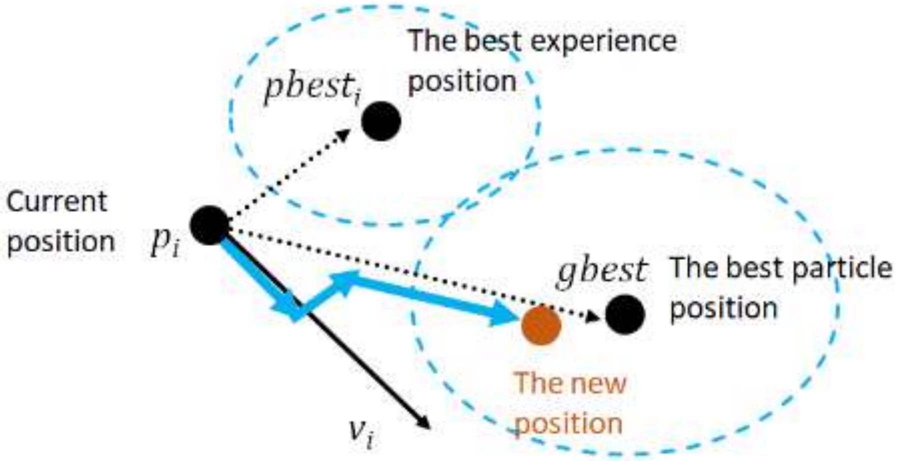

Figure 2. The process of Enhanced Particle Swarm Optimization

To surpass the constraints of classical optimization techniques in handling multiparameter, strong coupling, and nonlinear engineering optimization problems, the EPSO preserves population variety and improves information transfer across populations during optimization. These drawbacks included the propensity to quickly enter local optimization and advanced convergence. The concept of parameter selection for efficiency is established by analyzing the variables included in the integrated "local-global information sharing" phrase. Finally, to confirm the EPSO's global search efficiency, several sets of classical functions are employed to test the efficacy of the EPSO and conventional optimization techniques.

The objective of this work is to present an EPSO variation that attempts to enhance the PSO technique's efficiency in identifying better solutions while maintaining its simplicity and quick convergence. This distraction element stems from the addition of a new, straightforward operation to the iterative search procedure, which improves the method's capacity to discover and utilize intermediate solutions as well as to explore new regions of the search space that might hold superior answers. A updated PSO version that depends on parameter settings serves as the foundation for the suggested variant.

- **Distraction factor**

When a text feature vector's dimensions are too high, the particles in PSO will congregate at a certain position before reaching the global optimum. In order to guarantee the best convergence, distraction factor K was incorporated into PSO. The velocity formula is shown in Formula (1):

$$v_{id} = K[v_{id} + c_1 \times rand() \times (p_{id} - x_{id}) + c_2 \times Rand() \times \left(p_{gd} - x_{id}\right)] \quad (3)$$

Value c1and value c2used 2.05which were the same with Clerc’s experiment. For this study, set aside four decimal places for K. The specific velocity as:

$$v_{id} = 0.7298 \times [v_{id} + 2.05 \times rand() \times (p_{id} - x_{id}) + 2.05 \times Rand() \times \left(p_{gd} - x_{id}\right) \quad (4)$$

To find the optimal solution's likely position in the early rounds of PSO, a particle must detect throughout a large range. To find the ideal point in subsequent rounds, it must evolve locally within a narrow range. As a result, K ought to take a bigger value early on and a lower value later on. K should concurrently decrease gradually to the minimum throughout a lengthier late stage time. The con-cave function coincides with this pattern of change.

The early iterations of the distraction factor should select a convex function to prevent premature convergence and allow the particles to discover the optimal solution over a wide range. To allow the distraction factor to gradually decrease to the lowest in order to foster local development, it should select a concave function during the late era. It guarantees that the method will converge. Formula (5) illustrates the functional distraction factor organizing based on the cosine function, in accordance with this principle:

$$K = \frac{\cos((\pi/G_{max})\times T)+2.5}{4} \quad (5)$$

here T is the number of iterations. Set G_{max}= 40, the changing curve of value K appeared. K's curve in the function is first a convex function and eventually becomes a concave function. The value K given in formula (1), and then formula (1) turns into formula (6). Formula (6) is described below: The figure3. illustrate the flowchart of EPSO.

$$v_{id} = \left(\frac{\cos((\pi\times T/G_{max}))\times 2.5}{4}\right) \times [v_{id} + 2\times rand() \times (p_{id} - x_{id}) + 2\times Rand() \times (p_{gd} - x_{id})] \quad (6)$$

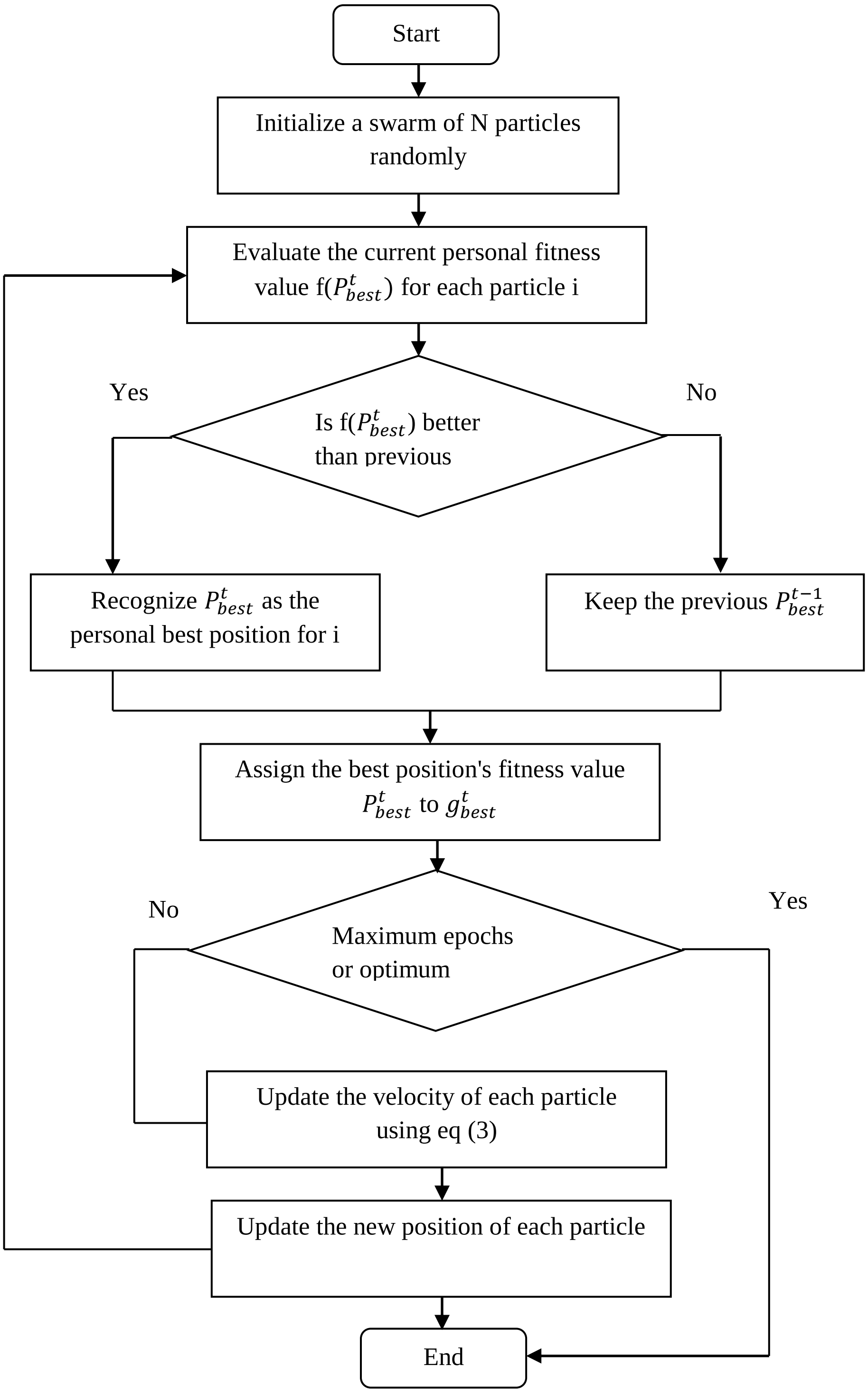
Start
Initialize a swarm of N particles randomly
Evaluate the current personal fitness value f(P^t_{best}) for each particle i
Yes
No
Is f(P^t_{best}) better than previous
Recognize P^t_{best} as the personal best position for i
Keep the previous P^{t-1}_{best}
Assign the best position's fitness value P^t_{best} to g^t_{best}
No
Yes
Maximum epochs or optimum
Update the velocity of each particle using eq (3)
Update the new position of each particle
End

figure 3. the flowchart of EPSO

Additionally, the structure's general robustness will be strengthened by implementing mechanisms to provide secure communication among local and global models. The suggested layout has potential applications in areas such as tracking employee productivity in businesses, which goes above e-learning. All things considered; the suggested structure offers a noteworthy advancement in tackling the difficulties associated with remote learning. Furthermore, the suggested design may find use in areas other than online learning, such tracking worker productivity in businesses.

4. Results and Discussion

The effectiveness of the proposed system is evaluated using the metrics namely accuracy, precision, recall f-measure. The proposed Federated Learning with Particle Swarm Optimization Algorithm (FLPSO)method is compared with the existing Privacy Preserving Federated Learning (PP-FL)andConvolution Privacy Preserving Algorithm (C-PPA). Here six federated model is used namely FedInspection V3, FedCNN, FedInspectionResnet V2, FedVGG16, FedVGG19 and FedResnet50.

- **Dataset**

Here, the nearly 4000 screenshots across five groups in the dataset were utilized.The primary goal of creating the dataset was to assess student productivity. Thus, the groups that are frequently utilized by students, those indicated in Table 1 have been selected:These courses were specifically picked since, in an e-learning environment, students might spend most of their time on computers, whether it be for programming, analyzing with Coursera or other e-sites, or watching YouTube tutorials. It is quite simple to become sidetracked by recommended videos when watching YouTube lessons, which leads to counterproductive viewing and the waste of important time. Because of this, all classes other than "Entertainment YouTube" count as productive. Consequently, if the screenshot is anticipated to be from one of these four classes, the time will be recorded in the log as effective; if the screenshot is estimated to come from the Entertainment YouTube class, the time will be recorded as unproductive.

Table 1. Description of dataset

Type of Class	Class	Size
Education Class	Education Coursera	800
	Education Google Classroom	799
	Education Programming	800
	Education YouTube	812
Entertainment Class	Entertainment YouTube	802

The table 1. shows the description of dataset. Utilizing a dataset of more than 4000 screenshots broken down into five classifications, the effectiveness of six alternative federated systems for identifying students' on-screen activities was assessed.

The ratio of successfully discovered positive findings to all predicted positive observations is known as precision.

$$Precision = TP/(TP + FP) \qquad (7)$$

The ratio of properly recognized positive findings to all data is known as sensitivity or recall.

$$Recall = TP/(TP + FN) \qquad (8)$$

The weighted average of both recall and precision is known as the F-measure. It requires false positives and negatives as an outcome.

$$F - measure = 2 * (Recall * Precision)/(Recall + Precision) \qquad (9)$$

The following formula determines accuracy regards to positives and negatives:

$$Accuracy = (TP + FP)/(TP + TN + FP + FN) \qquad (10)$$

Where TP- True Positive, TN-True Negative, FP-False Positive, FN- False Negative.

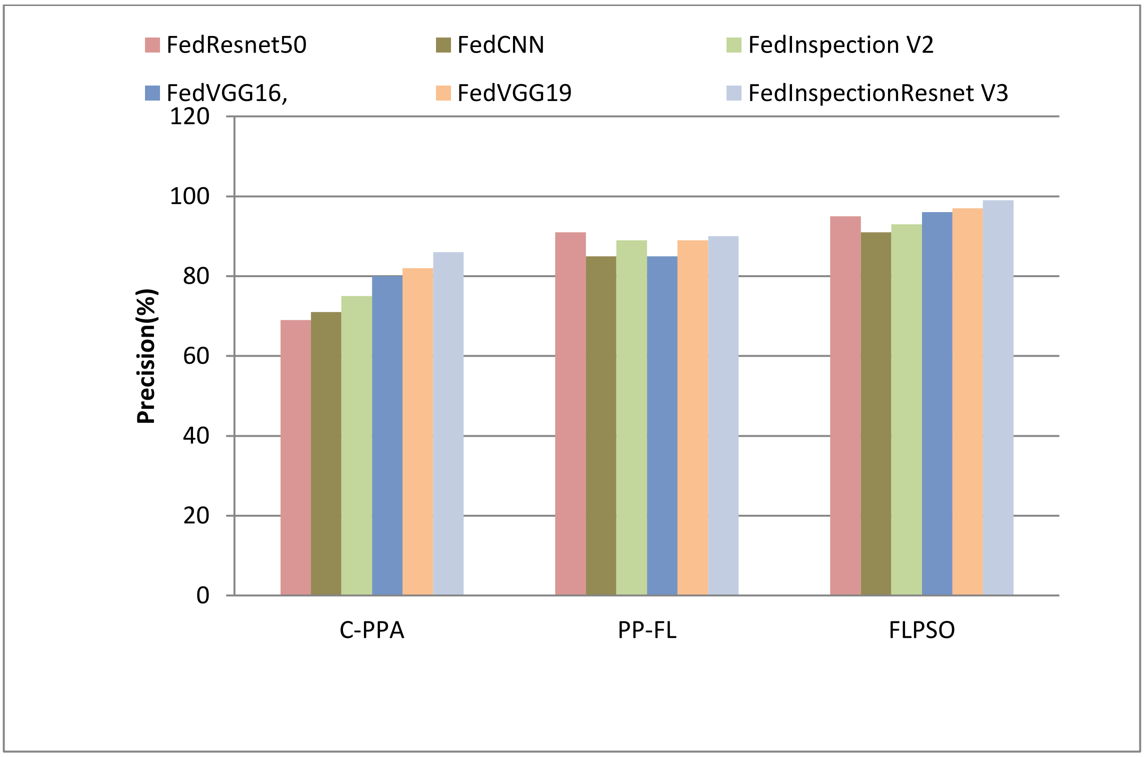

Fig.4. Precision comparison results between the proposed and existing method for activity recognition

Figure 4 shows the outcomes of a precision comparison among FLPSO and the current activity recognition technique. When the FLPSO system was contrasted to the other ML methods, outcomes showed that the FLPSO system performed better on the provided datasets. These findings are in line with the error rate that was previously obtained and can be linked to the rule sets that the FLPSO classification model developed. The findings indicate that, in comparison to other classification methods, the FLPSO technique produces results with a high degree of precision. Employ the macro precision metric in relation to the precision metric; it is computed by averaging the precision scores for all classes. The macro precision determines the precision for every class separately before averaging these scores without weight. Similar trade-offs, as FedResNet50 outperformed all other models, with FedRestNet50's values varying between 61.00% to 99.75% for FedInceptionV3. FedInceptionV3 achieved the maximum value of 99.75% in the weighted recall metric, while FedRestNet50 achieved the lowest value of 60.60%. This weighted recall metric followed the precision trend.

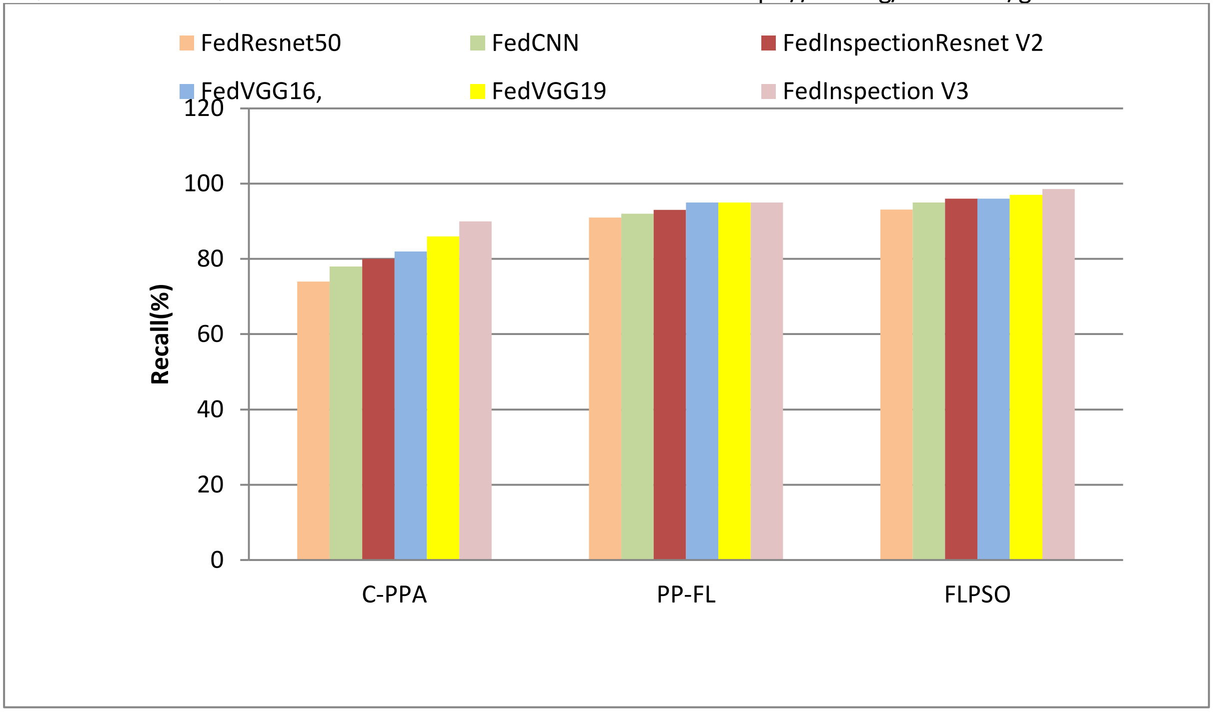

Fig.5. Recall comparison results between the proposed and existing method for activity recognition

Figure 5 shows the recall comparison findings for the suggested and current methods. The primary goal of the data utilized to categorize people employing screen pictures that include a variety of criteria that often influence their learning habits. Predictive models are therefore regarded as classification problems that arise from either the learner studied or not. As an outcome, the suggested FLPSO were employed for the assigned work, and the outcomes were examined and assessed. It was discovered that the Adam and SGD optimizers worked effectively with every model. During training, the optimizer is in charge of changing the model's parameters to minimize the loss function. The Adam optimizer, an SGD version, is renowned for its momentum and adaptable learning rate. It was discovered that Adam performed well in the FedVGG16 and FedVGG19 simulations, but SGD performed better in other approaches.

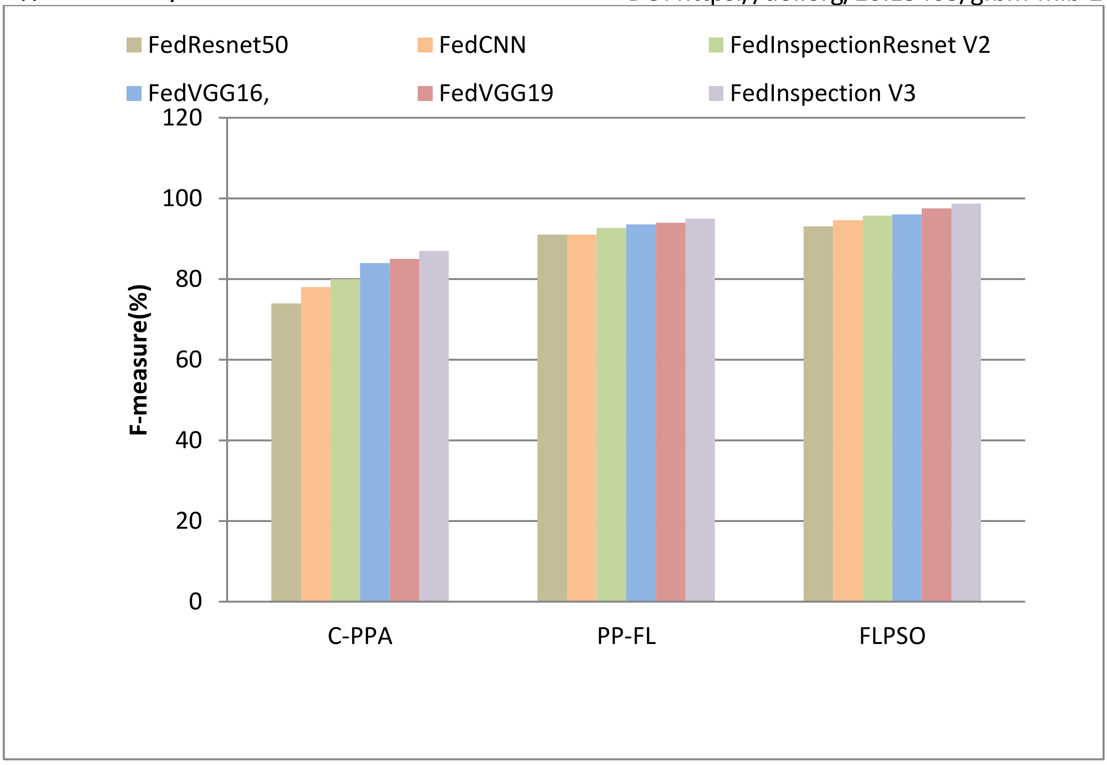

Fig.6. F-measure comparison results between the proposed and existing method for activity recognition

Figure 6 displays the outcomes of the F-measure comparison involving the suggested and current approach for identifying learners' activities. Moreover, there is a drastic decreasein the time required for performing a prediction when utilizing existing methods. When compared to the other frameworks, the comparison demonstrates that the suggested one has the greatest f-measure rate evaluation in the database. The database that was employed yielded the best f-measure findings. FedInceptionV3 earned the highest value of 99.75% according to the F1-score measure, which takes into account both precision and recall. FedCNN followed with 96.76%, Fed-VGG16 with 95.01%, FedVGG19 with 93.14%, FedInceptionResNetV2 with 94.26%, and FedRestNet50 with 57.00%.

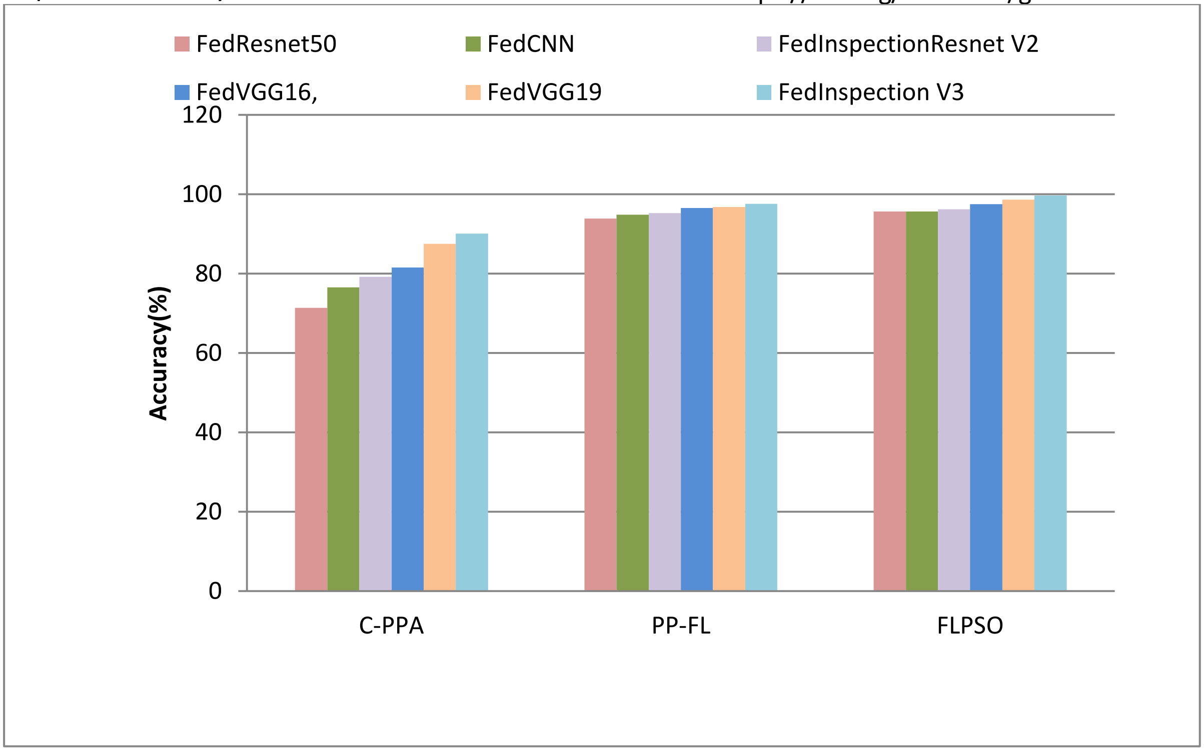

Fig.7. Accuracy comparison results between the proposed and existing method for activity recognition

Figure 7 shows the accuracy comparison among the suggested and current methods. A hybrid federated learning approach is considered effective if it can accurately anticipate the target and generalize predictions to new situations. In general, accuracy has two subtypes: sensitivity and specificity used to gauge the validity of the framework. From the simulation results it is identified that the proposed FLPSO model has high accuracy as 99.67% where as the existing PP-FL model has 93.9% and the C-PPA model has 71.41% respectively. According to the findings, the suggested FLPSO strategy outperforms the current classification methods in terms of accuracy. The graph's lines, each colored differently to reflect a distinct model, show the accuracy trends for each model. In general, the graph demonstrates that the FedInceptionV3 model outperforms the other methods with consistent accuracy, approaching near-perfect accuracy (close to 1) by the later epochs. Both FedCNN and FedVGG19 exhibit comparatively good accuracy scores, but with considerable variations over the training process. All models operate outstandingly with regard to of accuracy, with the exception of FedResNet50.

5. Conclusion

An inventive recommendation method for privacy-preserving educational technology is provided by this study. This smart computing framework is hybrid and design learning curricula according to the individual on-screen activities of each student. It is predicated on sophisticated federated learning methods for generating learning repositories through high-level privacy-preserving evaluations. The suggested structure for identifying pupils' on-screen behavior provides opportunities for future development and exhibits encouraging outcomes. The suggested smart framework, which constantly included the modeling challenges and uncertainty brought forth by the subjective learning framework, produced outstanding outcomes in every evaluation condition. Employing privacy-preserving recommendations to solve multidimensional and complicated issues is a significant innovation. The study has yielded an interesting discovery about the potential to apply techniques and completely theoretical computing to truly unstructured data, with fully accessible and practical outcomes. It is clear that FedInceptionV3 performs exceptionally well, classifying the samples with almost flawless accuracy. With certain deviations noted, the other methods likewise perform admirably with regard to of categorization accuracy. Interestingly, FedResNet50 seems to do less well than the other models overall. With FedResNet50 being the least successful system amongst them, these results demonstrate how well FedInceptionV3 and the other algorithms function in correctly classifying the test data.

REFERENCES

1. Villegas-Ch, W., Román-Cañizares, M., & Palacios-Pacheco, X. (2020). Improvement of an online education model with the integration of machine learning and data analysis in an LMS. *Applied Sciences*, *10*(15), 5371.
2. Shalev-Shwartz, S. (2012). Online learning and online convex optimization. *Foundations and Trends® in Machine Learning*, *4*(2), 107-194.
3. Villegas-Ch, W., Román-Cañizares, M., & Palacios-Pacheco, X. (2020). Improvement of an online education model with the integration of machine learning and data analysis in an LMS. *Applied Sciences*, *10*(15), 5371.
4. Kotsiantis, S. B., Pierrakeas, C. J., &Pintelas, P. E. (2003). Preventing student dropout in distance learning using machine learning techniques. In *Knowledge-Based Intelligent Information and Engineering Systems: 7th International Conference, KES 2003, Oxford, UK, September 2003. Proceedings, Part II 7* (pp. 267-274). Springer Berlin Heidelberg.
5. Moubayed, A., Injadat, M., Nassif, A. B., Lutfiyya, H., &Shami, A. (2018). E-learning: Challenges and research opportunities using machine learning & data analytics. *IEEE Access*, *6*, 39117-39138.
6. Sutton, R. S., & Whitehead, S. D. (2014, May). Online learning with random representations. In *Proceedings of the Tenth International conference on machine learning* (pp. 314-321).
7. Rasheed, F., & Wahid, A. (2021). Learning style detection in E-learning systems using machine learning techniques. *Expert Systems with Applications*, *174*, 114774.
8. Lu, D. N., Le, H. Q., & Vu, T. H. (2020). The factors affecting acceptance of e-learning: A machine learning algorithm approach. *Education Sciences*, *10*(10), 270.
9. Aher, S. B., & Lobo, L. M. R. J. (2013). Combination of machine learning algorithms for recommendation of courses in E-Learning System based on historical data. *Knowledge-Based Systems*, *51*, 1-14.
10. Tan, M., & Shao, P. (2015). Prediction of student dropout in e-Learning program through the use of machine learning method. *International journal of emerging technologies in learning*, *10*(1).
11. Khanal, S. S., Prasad, P. W. C., Alsadoon, A., &Maag, A. (2020). A systematic review: machine learning based recommendation systems for e-learning. *Education and Information Technologies*, *25*, 2635-2664.
12. Lykourentzou, I., Giannoukos, I., Nikolopoulos, V., Mpardis, G., &Loumos, V. (2009). Dropout prediction in e-learning courses through the combination of machine learning techniques. *Computers & Education*, *53*(3), 950-965.
13. Ghatasheh, N. (2015). Knowledge level assessment in e-learning systems using machine learning and user activity analysis. *International Journal of Advanced Computer Science and Applications*, *6*(4), 107-113.
14. Mihăescu, M. C. (2011, September). Classification of learners using linear regression. In *2011 federated conference on computer science and information systems (FedCSIS)* (pp. 717-721). IEEE.
15. Kushik, N., Yevtushenko, N., & Evtushenko, T. (2020). Novel machine learning technique for predicting teaching strategy effectiveness. *International Journal of Information Management*, *53*, 101488.
16. Anwar, M., & Greer, J. (2011). Facilitating trust in privacy-preserving e-learning environments. *IEEE Transactions on Learning Technologies*, *5*(1), 62-73.
17. Jegadeesan, S., Obaidat, M. S., Vijayakumar, P., Azees, M., &Karuppiah, M. (2022). Efficient privacy-preserving anonymous authentication scheme for human predictive online education system. *Cluster Computing*, *25*(4), 2557-2571.
18. Bagunaid, W., Chilamkurti, N., &Veeraraghavan, P. (2022). AISAR: Artificial Intelligence-Based Student Assessment and Recommendation System for E-Learning in Big Data. *Sustainability*, *14*(17), 10551.
19. Nagarathinam, T., Elangovan, V. R., Obaid, A. J., Akila, D., & Tuyen, D. Q. (2021, July). E-learning in data analytics on basis of rule mining prediction in DM environment. In *Journal of Physics: Conference Series* (Vol. 1963, No. 1, p. 012166). IOP Publishing.

20. Rodriguez-Garcia, M., Balderas, A., &Dodero, J. M. (2021). Privacy preservation and analytical utility of E-learning data mashups in the web of data. *Applied Sciences*, *11*(18), 8506.
21. Samad, A. A., Arshad, M. M., & Siraj, M. M. (2021, November). Towards Enhancement of Privacy-Preserving Data Mining Model for Predicting Students Learning Outcomes Performance. In *2021 IEEE International Conference on Computing (ICOCO)* (pp. 13-18). IEEE.
22. Ashwin, T. S., & Rajendran, R. (2023, June). Preserving Privacy of Face and Facial Expression in Computer Vision Data Collected in Learning Environments. In *International Conference on Artificial Intelligence in Education* (pp. 561-567). Cham: Springer Nature Switzerland.
23. Xu, S., & Yin, X. (2022). Recommendation system for privacy-preserving education technologies. *Computational Intelligence and Neuroscience*, *2022*.
24. Tajanpure, R., &Muddana, A. (2023). Data analysis with performance and privacy enhanced classification. *Journal of Intelligent Systems*, *32*(1), 20220215.
25. 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*.
26. Wang, D., Tan, D., & Liu, L. (2018). Particle swarm optimization algorithm: an overview. *Soft computing*, *22*, 387-408.
27. B. J. Ferdosi, M. Sadi, N. Hasan, and M. A. Rahman, ‘‘Tracking digitaldevice utilization from screenshot analysis using deep learning,’’ in *Proc.Int. Conf. Data Sci. Appl. (ICDSA)*, vol. 1. Singapore: Springer, 2023,pp. 661–670.