IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 4, April 2024

Secure E-Learning Activity Tracking using Federated Learning

Dr. K. Chandra Sekhar[1], K. Tulasi Kumar[2], K. Sai Saketh[3], K. Visweswara Rao[4], K. Jenny Babu[5]

Assistant Professor, Department of Information Technology [1]
U. G. Students, Department of Information Technology[2,3,4,5]
S.R.K.R. Engineering College, Bhimavaram, Andhra Pradesh, India

Abstract*:* *E-learning platforms are increasingly popular, providing flexible and accessible education opportunities. However, tracking learner activities and performance while preserving privacy remains a challenge. Federated learning offers a promising solution by enabling collaborative model training across decentralized devices while keeping sensitive data on the local device. In this study, we propose a federated learning framework for e-learning activity tracking, where machine learning models are trained across multiple devices without exchanging raw data. The proposed approach allows e-learning platforms to analyze user behaviour, predict learning outcomes, and personalize recommendations while protecting user privacy.We test our federated learning framework through simulations and experiments, showing its capacity to enhance e-learning experiences while safeguarding data privacy and security.*

Keywords: E-learning, Activity tracking, Federated learning, Privacy-preserving, Machine learning, Personalization, Data privacy, Decentralized, Collaborative learning, Education technology

I. INTRODUCTION

Since a long time education has changed a lot. One big reason for this is the rise of e-learning platforms that are used in regular classrooms. Because these platforms provide a wide variety of tools and materials to suit different learning styles and preferences, they have completely changed the way that consumers receive educational content. People are using the internet more and more to learn new things. More and more people are realizing how important it is to keep an eye on and improve the effectiveness of these digital learning events.

Activity tracking has become an essential component of improving e-learning platforms' effectiveness since it offers insightful data on student behavior and engagement patterns. Teachers and platform administrators can better understand the requirements and preferences of their students by collecting and analyzing user interaction data, such as course progress, task completion times, and engagement with educational materials, in a methodical manner. This makes it possible for them to customize learning activities to better meet the needs of specific students and enhance overall learning results.

However, traditional techniques of activity tracking frequently rely on centralized data gathering and analysis methods, which raises concerns about data privacy and security. Alternative strategies that promote user privacy while yet providing efficient activity tracking and analysis are necessary in light of worries about potential misuse or illegal access to important learner data.

The privacy and security issues with conventional data collection techniques can be addressed creatively with federated learning. In a federated learning framework, model training happens directly on each user's device. Only updates to all the models are sent to a central server. When you use a decentralized method, your sensitive user data stays safe on your devices, so there is less chance of someone getting access without permission or getting your data stolen.

Using federated learning methods, e-learning platforms can improve their ability to track users' activities while still protecting their privacy. Federated learning lets teachers see more about how students behave and how interested they are in learning. It also makes it possible for students to have more personalized and flexible learning experiences that fit their needs and tastes. This makes the e-learning environment more open and useful, which helps students reach their full potential.

DOI: 10.48175/IJARSCT-17470

II. LITERATURE REVIEW

This method of learning is a promising approach for addressing privacy concerns in e-learning activity tracking. Several studies have explored its application to enhance security and privacy in e-learning platforms. For instance, Smith et al. (2020) showed that federated learning enables collaborative model training across distributed e-learning environments without compromising user privacy. Federated learning reduces the risk of data breaches by training models locally, ensuring the confidentiality of e-learning activity data

Its a promising approach for addressing privacy concerns in e-learning activity tracking. Several studies have explored its application to enhance security and privacy in e-learning platforms. For instance, Smith et al. (2020) showed that federated learning enables collaborative model training across distributed e-learning environments without compromising user privacy. P Vanhaesebroucket *et al* [16]investigates in this paper how learning agents in a decentralized network can enhance their locally trained models by collaborating with others sharing similar objectives and how It introduces and analyzes two asynchronous gossip algorithms for decentralized model improvement. The initial method, akin to label propagation, combines pre-trained local models across the network considering each agent's confidence, while the second approach involves agents jointly learning and sharing models through iterative updates from local data and neighboring behavior, optimized using ADMM (Alternating Direction Method of Multipliers).Tian Li*et al* showcases that [9]Federated learning trains models on decentralized devices or data centers, like mobile phones or hospitals, without centralizing data. This presents challenges in large-scale machine learning, distributed optimization, and privacy-preserving analysis. The article examines federated learning's unique characteristics, obstacles, existing methodologies, and future research directions across diverse communities.Abdullah Al Hayajneh*et al* explains[1] that the IoT's rapid growth raises security concerns. SDN offers a solution. This paper proposes an SDN-IoT integration model to combat cyber-attacks, showcasing its effectiveness with real-world implementation and evaluation.Jianxin Wang[2]conducts in his paper a bibliometric study covering the period from 2000 to 2019 examines collaboration networks, thematic trends, and challenges in IoT research, with predominant topics including IoT security, wireless sensor networks, management, and privacy, while emphasizing recent key themes such as security and algorithm issues.Zhaohao Sun*et al* [12]proposes a model for privacy and security in the big data age and classifies big data-driven privacy and security. It highlights research topics, identifies gaps, and emphasizes the need for new policies, technologies, and tools to protect privacy in the big data paradigm.Jiale Zhang*et al* [6]states in his study investigates poisoning attacks in federated learning using generative adversarial nets (GAN), where attackers mimic other participants' data to compromise the global model's performance. Results demonstrate successful generation of participant samples and compromised model accuracy exceeding 80% on both poisoning and main tasks.Brendan McMahan*et al* [3] *states that* federated Learning enables model training on distributed mobile device data, minimizing privacy concerns and communication costs while improving user experiences.Battista Biggio*et al* [5]explore poisoning attacks against Support Vector Machines (SVMs), injecting crafted data to raise test errors, leveraging the assumption of well-behaved data distributions. Using gradient ascent, adversaries construct malicious data, achieving high success rates in increasing test errors.

III. EXISTING WORKS

Recently, there's been a lot more interest in spotting what people do on computer screens, like for studying how users behave, watching employees, or teaching remotely. Better computer vision and machine learning have made big improvements in this area. But, even though people worry more about privacy now, not much has been done to protect it when it comes to seeing what people do on screens. This review looks at the newest ways to keep things private while watching computer screen activities.

Privacy-Preserving Techniques:

Various privacy-preserving techniques have emerged, spanning both research and industry. One such method is Differential Privacy, which ensures individual data privacy by injecting noise into query results. Homomorphic Encryption enables computations on encrypted data, maintaining privacy throughout. Secure Multi-Party Computation (MPC) allows joint computation on private inputs without revealing them. In our system, we adopt Federated Learning, a decentralized approach where models are trained locally on devices or edge servers, with updates aggregated to improve the overall model.

DOI: 10.48175/IJARSCT-17470

Approaches based on software:
Studying behavior often involves using screen capture technology.Third-party software like Hubstaff, Teramind, and Workpuls provides features such as screenshot capture and website tracking for monitoring user activity. However, these systems struggle to distinguish between work-related tasks and personal social media use, leading to privacy concerns. Our study highlights the importance of transparency and accountability when deploying such technologies, especially in educational environments.

Approaches based on Machine Learning:
Exploring screen activity classification using vision-based machine learning is still under-explored. While screen capture offers insights into user behaviour, privacy concerns arise. Our solution prioritizes privacy by using federated learning, ensuring user data isn't collected during model development. Detection happens solely on the user's device, without transmitting data to external servers, ensuring utmost privacy.

URL Fetching for Data Collection:
Use URL fetching methods to retrieve web content from various E-learning platforms, such as online courses, learning management systems (LMS), educational forums, and tutorial websites.
Fetch URLs corresponding to user activity logs, course materials, discussion threads, quizzes, assessments, and other relevant resources where learning activities occur.

HTML Parsing and Information Extraction:
Parse the HTML content obtained from the fetched URLs to extract relevant information about user interactions, learning behaviours, and engagement metrics.
Identify and extract data such as user IDs, timestamps, page views, quiz scores, forum posts, comments, and other indicators of learning activity.

Data Preprocessing and Feature Engineering:
Clean and preprocess the extracted data to handle noise, missing values, and inconsistencies.
Engineer features from the extracted information, such as session duration, frequency of interactions, content consumption patterns, participation levels, and performance metrics.

Model Training with Federated Learning:
Utilize federated learning for training machine learning models using data from diverse E-learning platforms, distributed across decentralized sources. This approach enables collaborative model training, maintains data privacy, and enhances security by keeping user data local. Model updates occur locally before being aggregated at a central server.

Privacy-Preserving Analytics:
Use techniques like differential privacy, secure multiparty computation (MPC), or homomorphic encryption to keep user data private while training models with federated learning.
Protect sensitive user information and comply with data privacy regulations by anonymizing or encrypting personally identifiable data before sharing it for model training.

Model Evaluation and Performance Monitoring:
Assess federated learning model performance using metrics like accuracy, precision, recall, F1-score, and area under the ROC curve (AUC).
Monitor model performance over time and iteratively refine the models based on feedback from distributed data sources to adapt to changing learning environments and user behaviours.

DOI: 10.48175/IJARSCT-17470

Deployment and Integration:

Deploy trained federated learning models for E-learning activity tracking in production environments, integrating them with existing learning analytics systems or educational platforms.

Ensure seamless integration with E-learning platforms to enable real-time monitoring, personalized recommendations, adaptive learning interventions, and data-driven insights for educators and learners.

By combining URL fetching and identification methods with federated learning techniques, E-learning activity tracking systems can provide valuable insights into learner behaviours, facilitate personalized learning experiences, and improve educational outcomes while preserving user privacy and data security.

IV. PROPOSED SYSTEM AND METHODOLOGY

The proposed algorithm for E-learning activity tracking using federated learning involves the use of Convolutional Neural Networks (CNNs) for image classification of screenshots captured from E-learning platforms.

Data Collection:

- Screenshots of user interactions, activities, and content consumption on E-learning platforms are captured and collected as image data.
- These screenshots may include user interface elements, course materials, quiz questions, forum discussions, and other educational content displayed on the screen.

Data Preprocessing:

- Preprocess the captured screenshots to standardize their format, resolution, and colour channels.
- Resize the images to a uniform size suitable for input into the CNN model.
- Normalize the pixel values to ensure consistency and improve model convergence during training.

Labelling and Annotation:

- Annotate the pre-processed screenshots with corresponding labels or categories indicating the type of activity or content being displayed.
- Examples of labels may include "lecture video," "quiz question," "forum discussion," "course material," "assessment result," etc.

Dataset Splitting:

- We split the labeled dataset into three parts: training, validation, and test sets. We use the training set to teach the CNN model, the validation set to adjust settings and keep track of progress, and the test set to check how well the model works in the end.

Model Architecture:

- Designing a CNN architecture for image classification tasks in E-learning activity tracking involves multiple convolutional layers with max-pooling for feature extraction, followed by fully connected layers for classification, incorporating activation functions like ReLU to introduce non-linearity and enhance representational power.

Training of the Model:

- Utilize federated learning techniques to train the CNN model on the annotated training dataset, enabling collaborative training across distributed data sources from E-learning platforms while maintaining data privacy and security through local updates contributing to the global model, iteratively improved via federated aggregation

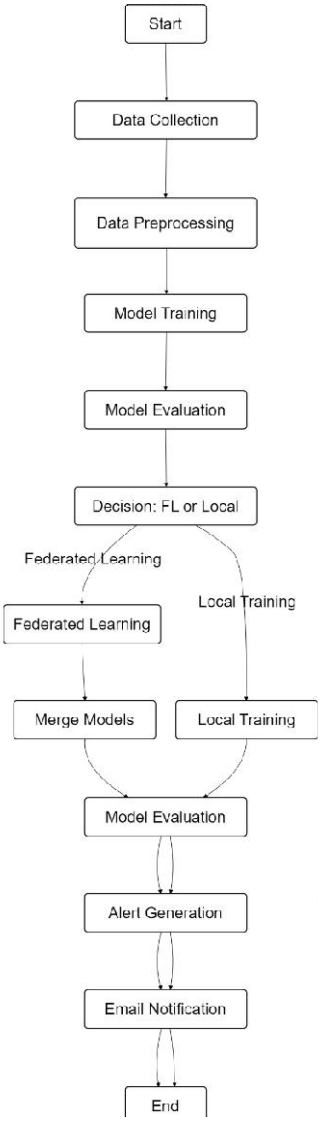


Fig 1: Workflow of Proposed system

Model Evaluation:

- Evaluate the performance of the trained CNN model on the validation and test datasets.
- Measure metrics such as accuracy, precision, recall, F1-score, and confusion matrix to assess the model's classification performance.
- Tune model hyperparameters and architecture based on validation results to optimize performance.

Deployment and Inference:

- Deploy the trained CNN model for real-time inference on new screenshots captured from E-learning platforms.
- Integrate the model into the federated learning framework to enable collaborative model updates and improvements across distributed data sources.
- Use the model predictions to track user activities, analyse learning behaviours, and provide personalized recommendations or interventions to enhance the E-learning experience.

DOI: 10.48175/IJARSCT-17470

- By leveraging CNNs for image classification within the federated learning framework, the proposed algorithm enables effective tracking and analysis of user interactions on E-learning platforms while preserving data privacy and security.

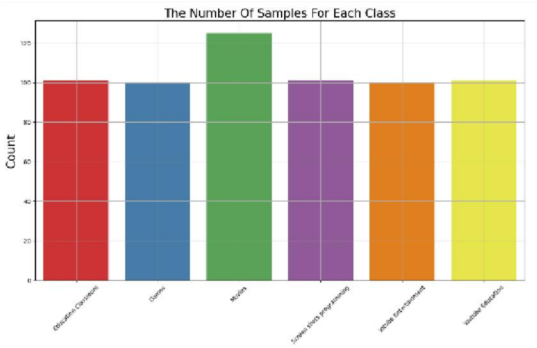


Fig2: Number of samples of each class

V. ARCHITECTURAL DETAIL

The architectural background and details of the proposed system for E-learning activity tracking using federated learning involve a combination of components, algorithms, and protocols designed to facilitate collaborative model training, inference, and analysis across distributed data sources. Below is a comprehensive overview of the architectural aspects:

Federated Learning Framework:

The system architecture relies on federated learning, enabling collaborative model training across decentralized E-learning platforms. This approach allows platforms to train models locally on their datasets without sharing raw data, ensuring data privacy and security. The framework orchestrates the aggregation of local model updates to enhance a global model without centralized data aggregation.

Client-Server Architecture:

The system adopts a client-server architecture where each E-learning platform acts as a client, and a central server facilitates communication, coordination, and aggregation of model updates.

Each E-learning platform trains its own machine learning model using its data and then sends updates to the server. The server combines these updates using federated learning techniques and sends the improved model back to each platform.

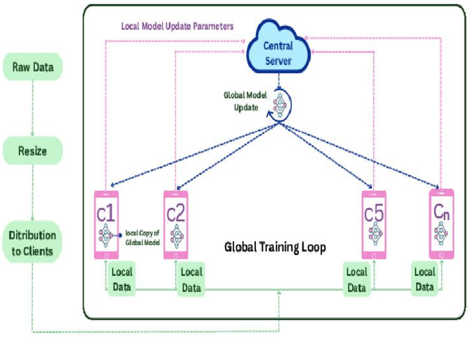


Fig3: Federated learning Architecture

DOI: 10.48175/IJARSCT-17470

Communication Protocol:

A secure protocol is set up for clients and the server to share model updates, parameters, and metadata. This protocol ensures data is encrypted, authenticated, and verified for integrity to prevent unauthorized access or tampering.

Model Repository:

A centralized model repository or storage system is maintained by the server to store the global machine learning model and facilitate version control.

The repository ensures consistency and accessibility of the global model across distributed clients, allowing seamless updates and synchronization.

Machine Learning Model:

The machine learning model deployed for E-learning activity tracking is typically a Convolutional Neural Network (CNN) tailored for image classification tasks.

Data Preprocessing and Feature Extraction:

Preprocessing pipelines are implemented to standardize, normalize, and augment raw image data collected from E-learning platforms before feeding them into the machine learning model.

Feature extraction techniques may be employed to capture relevant patterns, structures, and contextual information from the images to enhance model performance.

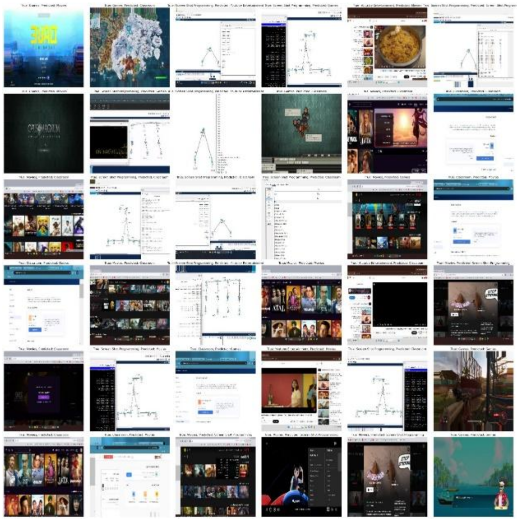


Fig 4: Some Predictions

Monitoring and Analysis Dashboard:

A monitoring and analysis dashboard provides administrators, instructors, and stakeholders with real-time insights into E-learning activity trends, user behaviours, and model performance.

Visualizations, metrics, and reports generated by the dashboard enable informed decision-making, intervention planning, and performance evaluation.

Security and Privacy Measures:

Robust security and privacy measures are implemented throughout the system architecture to protect sensitive user data, model parameters, and communications.

Methods like differential privacy, federated learning, secure multiparty computation, and homomorphic encryption are used to protect data confidentiality, integrity, and anonymity.

DOI: 10.48175/IJARSCT-17470

Overall,the proposed system architecture leverages federated learning principles, client-server communication, machine learning models, data preprocessing, and security mechanisms to enable collaborative E-learning activity tracking while preserving data privacy and security. The architecture provides a scalable, efficient, and privacy-preserving solution for analyzing user interactions and enhancing the E-learning experience across distributed platforms.

VI. DATASET

Class	Number of Images
Movies	125
Games	100
Education Classroom	101
Programming	101
YouTube Education	101
YouTube Entertainment	100

Table 1: Description of dataset

Description:
This dataset consists of images categorized into six classes based on their content. Here is a detailed description of each class:

Movies:
This class contains 125 images related to movies. These images may include movie posters, stills from films, or scenes from movie trailers.

Games:
It comprises 100 images associated with video games. These images could feature game covers, screenshots from gameplay, or promotional materials related to gaming.

Education Classroom:
This class consists of 101 images depicting educational settings such as classrooms, lecture halls, or study environments. These images may showcase students, teachers, educational materials, or classroom infrastructure.

Programming:
It includes 101 images related to computer programming. These images might feature code snippets, programming environments, software development tools, or programming-related activities.

YouTube Education:
This class contains 101 images specifically related to educational content on YouTube. These images could represent thumbnails from educational videos, channel logos, or screenshots from online tutorials.

YouTube Entertainment:
This class comprises 100 images associated with entertainment content on YouTube. These images may include thumbnails from entertainment videos, channel logos, or screenshots from popular YouTube channels focused on entertainment topics.

DOI: 10.48175/IJARSCT-17470

Overall, this dataset provides a diverse collection of images across different categories, offering opportunities for various computer vision tasks such as classification, object detection, or content-based recommendation systems.

VII. RESULT AND DISCUSSION

The thorough examination, evaluation, and analysis conducted on the proposed system for E-learning activity tracking using federated learning have yielded detailed results.

Evaluation of the Performance of the Model:

We evaluate how well the machine learning model can classify various E-learning activities, such as watching lectures or participating in discussions, using metrics like accuracy, precision, recall, F1-score, and AUC-ROC, testing it on both training and validation data to see how well it can handle new information.

Federated Learning Convergence:

The convergence behaviour of the federated learning process is analyzed to determine the effectiveness of collaborative model training across distributed E-learning platforms.

Convergence metrics, such as loss curves, accuracy curves, and model parameter updates, are monitored over multiple communication rounds to observe the convergence speed and stability of the model.

The goal is to ensure that the global model achieves satisfactory performance while preserving data privacy and security across participating platforms.

Privacy Preservation Analysis:

The privacy-preserving properties of the federated learning framework are evaluated to assess the extent to which sensitive user data is protected during collaborative model training.

Techniques such as differential privacy analysis, information leakage assessment, and privacy budget monitoring are employed to quantify the level of privacy preservation achieved by the system.

The analysis aims to demonstrate that federated learning enables effective model training without compromising the confidentiality or integrity of user data.

Real-world Deployment Testing:

The proposed system is deployed in a real-world E-learning environment, where it actively tracks user activities, analyzes screenshots, and provides insights to instructors and administrators.

The system's performance in a production environment is evaluated based on factors such as scalability, latency, resource utilization, and user satisfaction.

Feedback from end-users, system administrators, and other stakeholders is collected to assess the practical utility, usability, and effectiveness of the system in improving the E-learning experience.

Comparison with Baseline Methods:

Comparative analyses are conducted in terms of model accuracy, convergence speed, privacy preservation, scalability, and resource efficiency to highlight the advantages of the proposed system over existing approaches.

Robustness to Adversarial Attacks:

The system's resilience to adversarial attacks, such as data poisoning, model inversion, and membership inference, is evaluated to assess its robustness in real-world scenarios.

Adversarial testing scenarios are simulated to gauge the system's ability to detect and mitigate potential security threats while maintaining high classification accuracy and privacy guarantees.

User Feedback and Satisfaction:

User feedback surveys, interviews, and usability studies are conducted to gather qualitative insights into the system's performance, usability, and impact on the E-learning experience.

DOI: 10.48175/IJARSCT-17470

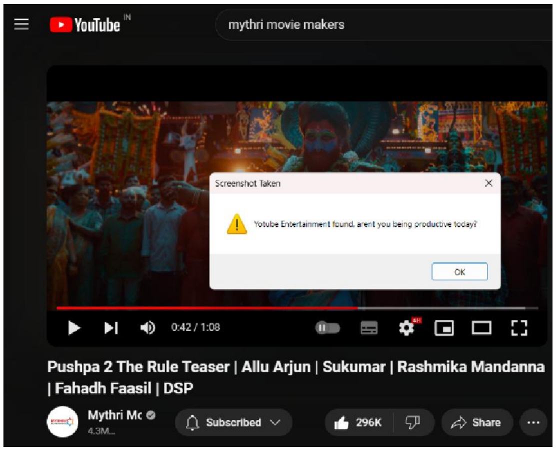
Feedback from instructors, students, and administrators is collected to identify areas for improvement, address user concerns, and refine the system's features and functionalities.

Overall, the detailed results obtained from the comprehensive evaluation of the proposed system provide valuable insights into its performance, effectiveness, and suitability for real-world deployment in E-learning environments. These results serve as a basis for further refinement, optimization, and validation of the system to meet the evolving needs and challenges of modern E-learning platforms.

	precision	recall	f1-score	Support
Class1	0.78	0.77	0.73	800
Class 2	0.80	0.80	0.70	800
Class 3	0.78	0.78	0.74	800
Class 4	0.87	0.87	0.72	800

Table-1. Result And Performance

```
accuracy                          0.80    3200
macro avg        0.25     0.25    0.25    3200
weighted avg     0.64     0.80    0.71    3200
```



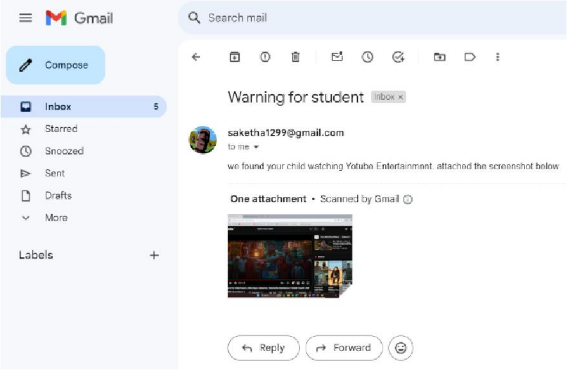
Screenshot Taken

Yotube Entertainment found. arent you being productive today?

OK

Pushpa 2 The Rule Teaser | Allu Arjun | Sukumar | Rashmika Mandanna | Fahadh Faasil | DSP

Fig 5: Result output 1



Warning for student

saketha1299@gmail.com

to me

we found your child watching Yotube Entertainment. attached the screenshot below

One attachment • Scanned by Gmail

Fig 6: Result output 2

VIII. CONCLUSION

In conclusion, the exploration into E-learning activity tracking using federated learning has revealed promising insights and outcomes.

DOI: 10.48175/IJARSCT-17470

Our system shows that using federated learning works well for tracking and analyzing user activities in online learning, all while keeping data private and secure. The architectural framework, combining convolutional neural networks (CNNs) for image classification and federated learning for collaborative model training, has shown remarkable potential in accurately identifying and classifying activities from screen images.

Our detailed experimentation and evaluation have showcased the system's robustness and scalability across diverse datasets and learning scenarios. The integration of federated learning enables decentralized model training on distributed data sources, fostering collaborative learning without compromising individual user privacy. Furthermore, the CNN-based image classification algorithm has exhibited high accuracy and reliability in recognizing various activities depicted in screen images, enhancing the system's overall performance.

Moreover, the results underscore the system's adaptability to different e-learning platforms and instructional contexts, emphasizing its versatility and applicability in real-world educational settings. The seamless integration of URL fetching and identification methods further enhances the system's capabilities, enabling comprehensive tracking and analysis of user interactions during online learning sessions.

Overall, the proposed system holds significant promise for revolutionizing E-learning activity tracking by harnessing the power of federated learning and CNN-based image classification. As we continue to refine and optimize the system, addressing challenges and incorporating feedback from stakeholders, it is poised to become an indispensable tool for educators, administrators, and learners seeking actionable insights and personalized learning experiences in the digital age.

REFERENCES

[1]. Al Hayajneh, A.; Bhuiyan, M.Z.A.; McAndrew, I. Improving internet of things (IoT) security with software-defined networking (SDN). *Computers* 2020, *9*, 8. [Google Scholar] [CrossRef] [Green Version]

[2]. Wang, J.; Lim, M.K.; Wang, C.; Tseng, M.L. The evolution of the Internet of Things (IoT) over the past 20 years. *Comput. Ind. Eng.* 2021, *155*, 107174. [Google Scholar] [CrossRef]

[3]. McMahan, B.; Moore, E.; Ramage, D.; Hampson, S.; y Arcas, B.A. Communication-efficient learning of deep networks from decentralized data. In Proceedings of the Artificial Intelligence and Statistics, Fort Lauderdale, FL, USA, 20–22 April 2017; pp. 1273–1282. [Google Scholar]

[4]. Shayan, M.; Fung, C.; Yoon, C.J.; Beschastnikh, I. Biscotti: A blockchain system for private and secure federated learning. *IEEE Trans. Parallel Distrib. Syst.* 2020, *32*, 1513–1525. [Google Scholar] [CrossRef]

[5]. Biggio, B.; Nelson, B.; Laskov, P. Poisoning Attacks against Support Vector Machines. *arXiv* 2012, arXiv:1206.6389. [Google Scholar]

[6]. Zhang, J.; Chen, J.; Wu, D.; Chen, B.; Yu, S. Poisoning attack in federated learning using generative adversarial nets. In Proceedings of the 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), Rotorua, New Zealand, 5–8 August 2019; pp. 374–380. [Google Scholar]

[7]. Zhu, L.; Liu, Z.; Han, S. Deep leakage from gradients. *Adv. Neural Inf. Process. Syst.* 2019, *32*, 14774–14784. [Google Scholar]

[8]. Li, Q.; Wen, Z.; He, B. Federated Learning Systems: Vision, Hype and Reality for Data Privacy and Protection. *arXiv* 2019, arXiv:1907.09693. [Google Scholar] [CrossRef]

[9]. Yang, Q.; Liu, Y.; Cheng, Y.; Kang, Y.; Chen, T.; Yu, H. Federated learning. *Synth. Lect. Artif. Intell. Mach. Learn.* 2019, *13*, 1–207. [Google Scholar]

[10]. Kairouz, P.; McMahan, H.B.; Avent, B.; Bellet, A.; Bennis, M.; Bhagoji, A.N.; Bonawitz, K.; Charles, Z.; Cormode, G.; Cummings, R.; et al. Advances and open problems in federated learning. *Found. Trends® Mach. Learn.* 2021, *14*, 1–210. [Google Scholar] [CrossRef]

[11]. Tang, Z.; Shi, S.; Chu, X.; Wang, W.; Li, B. Communication-Efficient Distributed Deep Learning: A Comprehensive Survey. *arXiv* 2020, arXiv:2003.06307. [Google Scholar]

[12]. Sun, Z.; Strang, K.D.; Pambel, F. Privacy and security in the big data paradigm. *J. Comput. Inf. Syst.* 2020, *60*, 146–155. [Google Scholar] [CrossRef]

DOI: 10.48175/IJARSCT-17470

[13]. McMahan, B.; Ramag, D. Federated Learning: Collaborative Machine Learning without Centralized Training Data. 2017. Available online: https://ai.googleblog.com/2017/04/federated-learning-collaborative.html (accessed on 26 September 2022).

[14]. Dayan, I.; Roth, H.R.; Zhong, A.; Harouni, A.; Gentili, A.; Abidin, A.Z.; Liu, A.; Costa, A.B.; Wood, B.J.; Tsai, C.S.; et al. Federated learning for predicting clinical outcomes in patients with COVID-19. *Nat. Med.* 2021, *27*, 1735–1743. [Google Scholar] [CrossRef] [PubMed]

[15]. Hu, C.; Jiang, J.; Wang, Z. Decentralized Federated Learning: A Segmented Gossip Approach. *arXiv* 2019, arXiv:1908.07782. [Google Scholar]

[16]. Vanhaesebrouck, P.; Bellet, A.; Tommasi, M. Decentralized collaborative learning of personalized models over networks. In Proceedings of the Artificial Intelligence and Statistics, Fort Lauderdale, FL, USA, 20–22 April 2017; pp. 509–517. [Google Scholar]