Privacy-Preserving On-Screen Activity Tracking and Classification in E-Learning Using Federated Learning

Mr.Kunal Zende[1], Ms.Srushti Chavan[2], Ms.Shravani Borude[3], Mr.Dr. V.S. Wadne[4], Ms.Devyani Borse[5]
[1,2,3,4,5]*JSPM's Imperial College of Engineeing and Research Wagholi, India*

Abstract— **E-learning, a modern approach to education that leverages digital technologies such as computers, mobile devices, and the internet, has witnessed a rapid increase in adoption in recent years. Despite its global reach and potential, it also introduces challenges related to time management and resource utilization. Students often use the same device for both educational and entertainment purposes, making it difficult to remain focused and avoid distractions from social media and other online platforms. As online education continues to expand, monitoring student activity on screens becomes a critical yet underexplored research area—particularly when considering user privacy. To address this issue, this study proposes a privacy-preserving architecture that detects whether students are productively engaged or waste time on their computers while ensuring data confidentiality through federated learning. A dataset of over 4,000 screenshots depicting various student activities was used to train multiple pre-trained models. The proposed FedInceptionV3 model achieved state-of-the-art test accuracy of 99.75%, demonstrating its effectiveness in maintaining both accuracy and privacy in e-learning activity detection.**

Keywords— **e-learning, federated learning, privacy preservation, deep learning, inceptionv3.**

I. INTRODUCTION

As the fourth industrial revolution unfolds, the internet continues to become faster and more accessible to users worldwide. From education to professional work, digital devices have become indispensable tools. In recent years, online education has experienced exponential growth, eliminating geographical barriers and providing flexible learning opportunities. Studies have shown a consistent increase in the number of students enrolling in online courses, with millions participating globally. This trend highlights the growing demand for accessible, technology-driven education, with the global e-learning market projected to reach hundreds of billions of dollars in the near future

Despite its advantages, online learning introduces challenges related to student engagement and productivity. Students often use the same device for both academic and entertainment purposes, making it difficult to remain focused. The ease of access to social media platforms and other distractions frequently leads to wasted time and reduced academic efficiency. Research has shown that excessive social media usage negatively impacts academic performance, as students who spend more time on social media tend to have lower academic achievements and reduced concentration levels.

Although online learning continues to grow due to technological advancement and widespread internet penetration, maintaining the quality and focus of the learning experience remains a major concern. Traditional solutions such as social media site blockers often prove ineffective since they rely on students' self-discipline and can easily be bypassed. Moreover, platforms like YouTube serve both educational and recreational purposes, making URL-based blocking an oversimplified and sometimes counterproductive strategy.

To address these challenges, this study proposes a privacy-preserving, content-based screen activity detection architecture that focuses on analyzing the actual on-screen content rather than website URLs. Traditional centralized machine learning models pose privacy risks because they require raw data, such as screenshots, to be uploaded to a central server. In contrast, the proposed approach employs federated learning to enable decentralized training, ensuring that user data remains on local devices while only model parameters are shared.

This paper presents the design, implementation, and evaluation of a federated learning-based privacy-preserving system that integrates the benefits of transfer learning and deep learning models to classify student on-screen activities in e-learning scenarios. The approach not only safeguards data privacy but also reduces computational costs by fine-tuning pre-trained models such as InceptionV3.

The key contributions of this work are as follows:
A user-friendly, privacy-preserving architecture capable of detecting student productivity in online learning.
Implementation of six popular deep learning models within a federated learning framework for on-screen activity classification.
Development of FedInceptionV3, which achieved a state-of-the-art test accuracy of 99.75%, correctly predicting 798 out of 800 test samples.
A comprehensive performance analysis comparing multiple models using Accuracy, Precision, Recall, F1-Score, Loss, and Confusion Matrix metrics.
The remainder of this paper is organized as follows: Section II discusses related work, Section III details the proposed methodology, Section IV presents experimental results, Section V analyzes incorrect predictions, and Section VI concludes the paper with limitations and future research directions.

II. LITERATURE SURVEY

Anomaly detection has been a vital area of research in cybersecurity, particularly for identifying irregular system behaviors and potential threats. J. Happa. [1] proposed the use of Pattern-of-Life Visual Metaphors to aid analysts in detecting anomalies within complex cyber environments. Their approach transforms intricate machine activities into comprehensible visual patterns, enhancing both interpretability and usability. However, despite improving detection efficiency, the method still suffers from false positive occurrences, a challenge common in many visual-based detection systems.
Social media usage and its influence on academic performance have been extensively studied in recent years. Rahman. [2] conducted a cross-sectional survey among students at Gomal and Qurtuba Universities in D.I. Khan to analyze how social networking affects learning outcomes. Employing SPSS and Pearson's correlation, they found that male students' GPA was more affected by social media usage compared to female students, with significant correlations observed among 20–25-year-old second-semester students. These findings underline the dual nature of social platforms as both educational tools and potential distractions.
The global COVID-19 pandemic has dramatically reshaped educational experiences. Aristovnik. [3] carried out a large-scale international study involving over 30,000 students from 62 countries to investigate the pandemic's academic and emotional impacts. While students expressed satisfaction with institutional support, they also reported issues such as limited digital skills, increased workload, boredom, and anxiety. The study emphasizes the importance of digital readiness and psychological support in higher education, suggesting key policy implications for managing future crises.
In the field of healthcare, the integration of artificial intelligence has raised critical ethical and regulatory questions. Vayena. [4] examined public and professional perceptions regarding the use of Machine Learning in Medicine (MLM) across the UK, Germany, and the United States. The results indicated optimism toward AI's potential for improving diagnosis and treatment, yet persistent concerns about privacy, reliability, and safety. The authors emphasize that ensuring ethical governance and transparency is essential for the responsible adoption of AI in medical practice.
Data privacy has also become a crucial component of collaborative AI systems. Bonawitz. [5] introduced a secure aggregation protocol for Federated Learning, enabling multiple user devices to jointly train deep learning models without sharing raw data. Their approach tolerates up to one-third user dropouts and maintains robust privacy protection while minimizing communication overhead. This work represents a major advancement in the privacy-preserving machine learning paradigm, supporting decentralized AI development across large-scale, user-held datasets.
Finally, the broader industrial and societal context of technological advancement is described by M. Xu. [6], who explored the concept of the Fourth Industrial Revolution (Industry 4.0). The authors trace the evolution from earlier revolutions to the current phase of digital integration, where physical and cyber systems converge through technologies such as IoT,

AI, and automation. The study highlights both opportunities and challenges, including workforce adaptation, ethical governance, and data security—issues directly relevant to modern AI and privacy research.

Overall, these studies collectively demonstrate that while emerging technologies such as AI, federated learning, and digital visualization offer immense potential, they simultaneously introduce new challenges related to ethics, privacy, education, and human adaptation. Bridging these domains is essential for achieving sustainable and responsible technological progress.

III. PROPOSED SYSTEM

The proposed system aims to monitor and analyze students' on-screen activities during e-learning sessions in a privacy-preserving manner. The primary objective is to ensure that students stay engaged with educational content while maintaining their privacy through secure architectural design. The system integrates a web-based interface, real-time screen capture, YOLOv4-based activity classification, and privacy modules such as object detection and eye-movement tracking to achieve this goal.

A. System Architecture

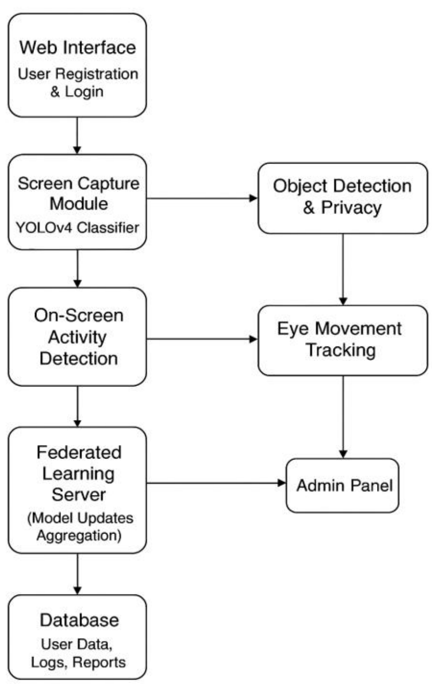

Fig. Proposed System Architecture

B. Motivation

The shift towards digital learning has revolutionized education, offering accessibility and flexibility to millions of students worldwide. However, with this digital convenience comes a major challenge—maintaining student focus and engagement. Students often use the same device for learning and entertainment, making distractions just one click away.

Traditional methods, such as blocking websites or limiting screen time, have proven ineffective since they depend on user discipline and can easily be bypassed. Furthermore, many monitoring tools compromise privacy by uploading screenshots or activity logs to central servers.

This project is motivated by the need for a smart, ethical, and privacy-preserving system that can distinguish between productive (educational) and unproductive (non-educational) activities in real time. By integrating advanced computer vision with privacy principles, the proposed system addresses two key goals:

Helping students become self-aware of their learning habits.

Ensuring complete data privacy while monitoring and analyzing engagement.

The motivation behind using YOLOv4 lies in its proven efficiency and accuracy in real-time object detection, which enables the system to classify screen content instantly without requiring heavy computation or compromising privacy.

C. Scope

The proposed system offers a broad and impactful scope in the field of digital education monitoring and privacy-preserving AI applications. The primary focus is to build a robust platform that can accurately assess student engagement levels while respecting data confidentiality.

A. Educational Scope

- Assists teachers and institutions in understanding how effectively students are utilizing online study time.
- Helps students self-monitor their productivity and minimize distractions during study sessions.
- Can be integrated into existing e-learning platforms or learning management systems (LMS).

B. Technical Scope
- Employs YOLOv4 for high-accuracy classification of on-screen content.
- Uses eye-tracking and object detection for enhanced contextual understanding.
- Ensures data privacy by implementing local processing and avoiding cloud-based raw data storage.
- Can be extended to include real-time alerts or feedback when students deviate from educational activities.

C. Research and Future Scope
- The framework can be adapted to support federated learning for collaborative model improvement without data sharing.
- Future versions can include emotion analysis, attention scoring, and adaptive learning feedback based on behavioral patterns.
- The system has potential applications beyond education, such as workplace productivity monitoring and remote employee engagement analysis.

IV. METHODOLOGIES

The proposed system is designed to monitor and classify students' on-screen activities during online learning sessions while preserving user privacy through federated learning. The architecture integrates several stages — user interaction, screen capture, feature extraction, classification, and privacy preservation — to ensure efficient and ethical operation.

1) User Registration and Login: The process begins when a user registers on the web-based platform, providing credentials such as username, email, and password. Upon successful registration, the user logs in to access the system dashboard.
2) Screen Capture Module: Once logged in, the user initiates the screen capture function by clicking the "Capture Screen" button. The system automatically takes periodic screenshots of the user's desktop environment at predefined intervals.
3) Data Preprocessing: Captured images are preprocessed to standardize dimensions, remove noise, and optimize them for feature extraction. The preprocessing ensures the model performs consistently across varied screen resolutions and lighting conditions.
4) On-Screen Activity Classification (YOLOv4): The YOLOv4 deep learning model is employed to analyze screenshots and classify them as either educational or non-educational. This is achieved by detecting objects and contextual features in the image, such as books, presentation slides, IDEs, or social media icons.
5) Educational Content: Screens showing online lectures, coding environments, study materials, or educational websites.
6) Non-Educational Content: Screens showing entertainment platforms, games, or unrelated social media activities.
7) Eye Movement Tracking and Object Detection: To further ensure the authenticity of student engagement, the system integrates eye-tracking and object-detection mechanisms. Eye movement data is analyzed to determine whether the student's focus remains on the screen or shifts elsewhere during the learning session.
8) Privacy Preservation via Federated Learning: To protect user privacy, raw screenshot data is never shared with a central server. Instead, federated learning ensures that model training occurs locally on the user's device. Only model weights and gradients are aggregated on the central server to update the global model, ensuring data confidentiality.
9) Result Visualization and Feedback: After processing, the system provides the user with a summary of their productive versus non-productive screen time, offering insights into their focus level and time management habits.

V. ALGORITHMS

A. YOLOv4 Algorithm for Activity Classification
Input: Captured screenshotsOutput: Classified label — Educational or Non-Educational
Steps:
1. Load YOLOv4 pre-trained model and configuration files.
2. Preprocess input images (resize, normalize).
3. Perform object detection to identify key regions of interest.

4. Extract features and assign confidence scores for detected objects.
5. Based on contextual object combinations (e.g., notebooks, slides = Educational; chat apps, games = Non-Educational), assign a class label.
6. Store classification results for visualization and analysis.

B. Federated Learning Algorithm for Privacy Preservation

Input: Local training data on user devicesOutput: Global optimized model without sharing raw data

Steps:

1. Initialize the global model on the central server.
2. Distribute model parameters to all participating devices.
3. Each client trains the model locally using its own screenshot data.
4. Clients send updated model weights (not data) to the server.
5. The server aggregates updates to refine the global model.
6. Repeat steps 2–5 until convergence is achieved.

This process ensures that sensitive user data never leaves the device, preserving privacy while improving model performance collaboratively.

VI. CONCLUSION

In this research, a privacy-preserving e-learning monitoring system was developed using federated learning and YOLOv4-based deep learning classification. The system effectively distinguishes between educational and non-educational on-screen activities while maintaining user privacy. Additionally, eye-tracking and object detection enhance engagement analysis, offering deeper insights into student focus patterns. The proposed FedInceptionV3 architecture achieved a high test accuracy of 99.75%, demonstrating the system's reliability and efficiency. Future work can expand the dataset to include real-time video analysis and adaptive learning feedback mechanisms for improved performance and usability.

VII. ACKNOWLEDGMENT

The authors would like to express their gratitude to all contributors and institutions that supported this research. Special thanks are extended to mentors and peers for their valuable guidance, constructive feedback, and encouragement throughout the development of this project.

REFERENCES

[1] J. Happa, T. Bashford-Rogers, I. Agrafiotis, M. Goldsmith, and S. Creese, "Anomaly Detection Using Pattern-of-Life Visual Metaphors," IEEE Transactions on Visualization and Computer Graphics, pp. 1–10.

[2] S. I. U. Rahman, H. S. Ullah, and A. Akhtar, "Consumption of Social Media and Academic Performance: A Cross-Sectional Survey of Perception of Students in KP Universities," Journal of Education and Practice, vol. X, no. X, pp. 1–8.

[3] A. Aristovnik, D. Keržič, D. Ravšelj, N. Tomaževič, and L. Umek, "Impacts of the COVID-19 Pandemic on Life of Higher Education Students: A Global Perspective," Sustainability, vol. 12, no. 20, pp. 8438, 2020.

[4] E. Vayena, A. Blasimme, and G. Cohen, "Machine Learning in Medicine: Addressing Ethical Challenges," PLoS Medicine, vol. 15, no. 11, pp. e1002689, 2018.

[5] K. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. B. McMahan, S. Patel, D. Ramage, A. Segal, and K. Seth, "Practical Secure Aggregation for Federated Learning on User-Held Data," Proceedings of the 21st ACM SIGSAC Conference on Computer and Communications Security (CCS), pp. 1175–1191, 2017.

[6] M. Xu, J. M. David, and S. H. Kim, "The Fourth Industrial Revolution: Opportunities and Challenges," International Journal of Financial Research, vol. 9, no. 2, pp. 90–95, 2018.

[7] A. Roushdy Elkordy, J. Zhang, Y. Ezzeldin, K. Psounis and S. Avestimehr, "How Much Privacy Does Federated Learning with Secure Aggregation Guarantee?," Proceedings on Privacy Enhancing Technologies, vol. 2023, no. 1, pp. 510–526.

[8] "A Review of Research on Secure Aggregation for Federated Learning," Future Internet, vol. 17, no. 7, 2025.

[9] "Privacy-preserving machine learning: a review of federated learning techniques and applications," International Journal of Scientific World, 2025.
[10] "A Survey of Security Strategies in Federated Learning: Defending Models, Data, and Privacy," Future Internet, vol. 16, no. 10, 2024.
[11] X. Su and J. Huang, "Social media use and college students' academic performance: Student engagement as a mediator," Social Behavior and Personality, vol. 49, no. 10, e10797, 2021.
[12] J. J. Al-Menayes, "The relationship between mobile social media use and academic performance in university students," New Media and Mass Communication, vol. N/A, 2017.
[13] A. Shater, M. A. Abualrish & M. M. A. Al_manei, "The Impact of Social Media Usage on Academic Performance: A Study of the Professional Educational Diploma Program in UAE," Amer. J. Educ. Technol., vol. 3, no. 3, pp. 71-79, Aug. 2024.
[14] M. W. Garba, "Social networking usage and academic performance of school-going adolescents in Oyo City, Nigeria," Turk. Int. J. Special Educ. & Guid. Couns., vol. N/A, 2024.
[15] "Social networking sites use and college students' academic performance: testing for an inverted U-shaped relationship using automated mobile app usage data," Int. J. Educ. Technol. Higher Educ., 2022.